LevelOne

WAP-0006/0009

11g Wireless AP

Bedienungsanleitung

V1.0-0609

Sicherheitshinweise

Lesen Sie vor der Inbetriebnahme dieses Wireless Acces Points die gesamte Bedienungsanleitung. Digital Data Communications GmbH übernimmt keine Haftung bei Sach- oder Personenschäden und etwaiger Folgeschäden, die infolge Nichtbeachtens dieser Bedienungsanleitung zustande kommen. Sie verlieren in diesem Fall Ihren Garantieanspruch.

Bestimmungsgemäße Verwendung

Dieser Wireless Access Point ist nur für den privaten, sowie den Einsatz in kleineren und mittleren Büros entwickelt worden.

Bestimmungswidrige Verwendung

- Dieser Wireless Acces Point ist nicht für die Verwendung in sicherheitssensiblen Umgebungen (z. B. Banken, Krankenhäuser, Flughäfen, Sicherheitseinrichtungen u.ä.) bestimmt.
- Er darf nicht in Umgebungen eingesetzt werden, die eine ständige Verfügbarkeit und Fehlerfreiheit, der IT-Systeme voraussetzen.
- Der Einsatz in Umgebungen in denen eine fehlerhafte, unsachgemäße oder missbräuchliche Anwendung zu materiellen Schäden (Finanz-, Wirtschafts- und Umweltschäden), Verletzungen, Todesfällen und anderen Schäden von Personen führen kann ist nicht bestimmungsgemäß.
- Das Öffnen des Gehäuses von Wireless Access Point und Steckernetzteil ist verboten. Durch Öffnen der Gehäuses und unsachgemäße Reparaturen können Gefahren für Sicherheit und Gesundheit des Benutzers, sowie unbeteiligter Personen entstehen.
- Die Digital Data Communications GmbH haftet nicht für Schäden die aus nicht bestimmungsgemäßer Verwendung resultieren.

Elektrische Spannung

- Dieser Wireless Access Point arbeitet intern mit 12 Volt Gleichspannung bei einer maximalen Leistungsaufnahme von etwa 6 Watt.
- Der Wireless Access Point ist nicht direkt mit dem 240 Volt Wechselspannungsnetz verbunden. Die Spannungsversorgung erfolgt über ein Steckernetzteil das die 240 Volt Wechselspannung in 12 Volt Gleichspannung umwandelt.
- Es dürfen keine Flüssigkeiten oder andere Gegenstände (z. B. Heftzwecken, Schrauben, Büroklammern u.ä.) in das Gehäuse des Wireless Acces Point und des Steckernetzteils gelangen. Es kann sonst die Gefahr eines Kurzschlusses entstehen.
- Legen Sie keine Gegenstände auf dem Wireless Access Point und dem Steckernetzteil ab.
- Der Betrieb des Wireless Acces Points ist nur mit dem mitgelieferten Steckernetzteil gestattet.

- Wireless Access Point und das mitgelieferte Steckernetzteil dürfen nur innerhalb von Gebäuden und in trockenen Räumen betrieben werden.

- Überzeugen Sie sich vor dem Einsatz des Wireless Access Point das die örtliche Spannungsversorgung mit den Werten auf dem Steckernetzteil (Bereich: 100-240 Volt, 50-60 Hz) übereinstimmt. Verbinden Sie Wireless Access Point, Steckernetzeil und Steckdose nur wenn die Angaben übereinstimmen. Falsche Spannungswerte können zur Überhitzung und damit zum Schmelzen des Steckernetzteilgehäuses führen. Es kann ein Brand entstehen.

- Öffnen Sie das Gehäuse des Steckernetzteils nicht, es besteht die Gefahr des elektrischen Schlages.
- Berühren Sie nicht die metallischen, spannungsführenden Kontakte, führen Sie keine metallischen Gegenstände in die Lüftungsschlitze des Steckernetzteils. Halten Sie das Steckernetzteil von Feuchtigkeit fern. Es besteht die akute Gefahr durch einen Stromschlag!

- Im Falle das Gehäuse, Kabel und Kontakte beschädigt sind, darf das Steckernetzteil nicht mehr verwendet werden. Es besteht die akute Gefahr durch einen Stromschlag!

- Im Falle eines Defektes nehmen Sie, zum Austausch des Steckernetzteiles, Kontakt mit Ihrem Händler oder der Hotline des Herstellers auf.

- Der Wireless Access Point, mit seinem Steckernetzteil darf nur an einer geerdeten Steckdose (Schukosteckdose, 3-polig) betrieben werden. Es dürfen keine Adapterstecker oder Verlängerungskabel verwendet werden.

- Ziehen Sie nicht am Anschlusskabel des Steckernetzteils!

- Verbinden Sie zuerst das Steckernetzteil mit dem Wireless Access Point, dann erst das Steckernetzteil mit der Steckdose.

- Um denn Wireless Access Point vom Stromnetz zu trennen, entfernen Sie zuerst die Verbindung von Steckernetzteil und Steckdose. Fassen Sie nicht die Kontakte des Steckernetzteils an, es besteht die Gefahr eines elektrischen Schlages! Dann trennen Sie die Verbindung zwischen Steckernetzteil und Wireless Access Point.

Überspannung

Installieren Sie den Wireless Access Point nicht während eines Gewitters. Stellen Sie keine Kabelverbindungen her. Trennen Sie während eines Gewitters Wireless Access Point und Steckernetzteil vom Stromnetz. Ein Blitzschlag kann in unmittelbarer Umgebung elektronische Geräte durch Überspannung beschädigen oder sogar zerstören. Hierdurch können Brände entstehen!

Kabelverbindungen

- Bevor Sie die Kabelverbindungen herstellen, beschriften Sie diese eindeutig, um eine Verwechselung zu vermeiden.

- Der LAN-Anschluß auf der Rückseite des Wireless Access Points darf nicht mit einer ISDN Telefon Anschlussdose verbunden werden. Der Wireless Access Point kann durch die bei ISDN übertragene Versorgungsspannung beschädigt werden. Bei Netzwerken und bei ISDN werden der gleiche Steckertyp (RJ-45) eingesetzt.

- Verwenden Sie nur Netzwerkanschlusskabel des Typs Kategorie 5 UTP und höher um die Brandgefahr zu mindern.

Einsatzort und Umgebungsbedingungen

Einsatzort

- Der Aufstellort muss ausreichend dimensioniert sein, um den Wireless Access Point waagerecht und sicher aufstellen zu können.

- Alle mit dem Wireless Access Point verbundenen Kabel sind so zu verlegen, das keine mechanische Belastung für die Kabel entstehen kann. Durch die Verlegung der Kabel darf keine Stolpergefahr entstehen.

- Die Steckdose, an der das Steckernetzteil angeschlossen ist, muss jederzeit gut erreichbar sein..
- Stellen Sie den Wireless Access Point so auf, dass die Stromversorgung des Steckernetzteils durch eine in der Nähe verfügbare Sicherheitssteckdose erfolgt. Diese Sicherheitssteckdose muss leicht zu erreichen sein, damit die Stromversorgung des Wireless Access Points im Notfall sofort abgeschaltet werden kann.

- Stellen Sie das Gerät nicht in der Nähe von Flüssigkeitsbehältern, wie Blumenvasen, Getränkeflaschen auf. So vermeiden Sie einen Kontakt des Gerätes, durch versehentliches Umkippen, mit der Flüssigkeit.

- Stellen Sie den Wireless Access Point außerhalb der Reichweite von Kindern und Haustieren auf.
- Das Gerät darf für Kinder und Haustiere nicht erreichbar sein!

Umgebungsbedingungen

- Stellen Sie den Wireless Access Point so auf, dass eine gute Belüftung von allen Seiten gewährleistet ist. Lassen Sie auf den Seiten der Lüftungsschlitze ausreichend Platz, so dass die Wärme schnell in den Raum abgeführt werden kann. Blockieren Sie nicht die Lüftungsschlitze!

- Setzen Sie den Wireless Access Point keiner direkten und starken Sonneneinstrahlung aus.

- Das Gehäuse kann sich sonst verformen, mit Bauteilen im Inneren in Kontakt kommen und so einen Brand verursachen.

- Stellen Sie den Wireless Access Point nicht auf oder direkt neben andere elektronische Geräte die sich selbst erwärmen. Eine für den Betrieb ausreichende Wärmeabfuhr ist dann nicht mehr gewährleistet. Es können Funktionsstörungen auftreten. Schalten Sie den Wireless Access Point für einige Minuten aus, entfernen Sie das Steckernetzteil aus der Steckdose.. Sorgen Sie nun für ausreichende Wärmeabfuhr und nehmen dann das Gerät erneut in Betrieb.

- Schützen Sie den Wireless Access Point und das Steckernetzteil vor Feuchtigkeit. Die Geräte dürfen unter keinen Umständen mit Wasser und anderen Flüssigkeiten in Verbindung kommen!

- Betreiben Sie den Wireless Access Point nur in dem Feuchtigkeitsbereich der in den Spezifikationen freigegeben ist.

- Der Wireless Access Point darf nicht in Bereichen wie Badezimmern, Küchen und anderen Feucht- Nass- und Trockenräumen betrieben werden. Betreiben Sie den Wireless Access Point nicht in der Nähe von Gebäudeöffnungen (Türen, Fenster) die einen Zugang nach außen haben, da plötzlich eintretender Regen unter Umständen in das Gerät eindringen kann.

Vorsichtsmaßnahmen zum Schutz von Kindern

Stellen Sie den Wireless Access Point so auf, dass er für Kinder nicht erreichbar ist.

Warnungen vor Schäden durch möglichen Fehlgebrauch

- Dieser Wireless Access Point darf nur mit dem mitgelieferten Steckernetzteil verwendet werden. Vermeiden Sie unter allen Umständen die ersatzweise Verwendung anderer Netzteile.

- Der Wireless Access Point darf nicht in Feuchträumen eingesetzt werden.

- Der Wireless Access Point darf nicht im Freien oder in halboffenen Bereichen (Veranda etc.) betrieben werden.

- Der Wireless Access Point und Steckernetzteil dürfen niemals mit Flüssigkeiten in Kontakt kommen.Sollte dies dennoch einmal geschehen, sofort die Stromzufuhr abschalten bzw. das Steckernetzteil aus der Steckdose ziehen. Gefahr durch Stromschlag! Lassen Sie vor erneuter Inbetriebnahme das Gerät durch einen Fachmann überprüfen!

- Der LAN-Anschluß auf der Rückseite des Wireless Access Points darf nicht mit einer ISDN Telefon Anschlussdose verbunden werden. Der Wireless Access Point kann durch die bei ISDN übertragene Versorgungsspannung beschädigt werden. Bei Netzwerken und bei ISDN werden der gleiche Steckertyp (RJ-45) eingesetzt. Eine Vertauschung ist somit nicht ausgeschlossen. Kennzeichnen Sie die Kabel, um einer Vertauschung vorzubeugen.

- Es dürfen keine physischen Veränderungen am Wireless Access Point oder am Steckernetzteil vorgenommen werden!

- Stecker und Steckernetzteil nicht am Kabel herausziehen und alle Kabel so verlegen, dass die Entstehung von Stolperfallen oder mechanischen Beschädigungen der Kabel ausgeschlossen sind!

Zielgruppe und Anforderungen auf Benutzerseite

Dieser Wireless Access Point ist ausgelegt für den Einsatz durch Computernutzer, die über hinreichende Fachkenntnis im Umgang mit einem Computer und in der Pflege eines kleinen Netzwerkes verfügen und die

mit der Nutzung dieses Wireless Access Points verbundenen Risiken und die Beachtung der Sicherheitshinweise gewährleisten können.

Für die Inbetriebnahme und Konfiguration des Wireless Access Points sind die folgenden Voraussetzungen und Kompetenzen erforderlich:

Sichere und verantwortliche Handhabung von elektrischen Geräten und Telekommunikationseinrichtungen. Kenntnisse über ihr eingesetztes Betriebssystem und drahtlose und drahtgebundene Netzwerke.

Wenn diese Voraussetzungen nicht erfüllt werden, sollte die Inbetriebnahme und Konfiguration durch Fachpersonal ausgeführt werden, um Risiken und mögliche Schäden infolge Fehlbedienung oder Fehlkonfiguration zu vermeiden.

Dieser Wireless Access Point ist nicht für Inbetriebnahme und Verwendung durch
• Menschen mit Behinderungen
• Senioren
• Kinder
vorbereitet und ausgelegt.

Schadensrisiken - Ausfall des IT-Systems

Bereits in kleinen Netzwerken kann der Ausfall einer einzigen Komponente, insbesondere an zentralen Knotenpunkten des Systems, zu einem Ausfall des gesamten Systems führen.

Wenn Sie Ihren Wireless Access Point als zentralen Knotenpunkt für Ihren lokalen Netzwerkverkehr verwenden, bewirkt ein Ausfall des Wireless Access Points, dass die im lokalen Netzwerk gespeicherten Daten und Geräte (z. B. Drucker) vorübergehend nicht zur Verfügung stehen.

Neben technischem Versagen und höherer Gewalt (z. B. Überspannung nach einem Blitzeinschlag) sind es häufig Bedienfehler bzw. menschliches Fehlverhalten, die für den Ausfall von IT-Geräten verantwortlich sind.

Vorsicht bei Firmware-Updates !

Führen Sie ein Update nur durch, wenn es für den Betrieb des Wireless Access Points unbedingt notwendig ist. Ein fehlerhaftes Update kann zum Ausfall Ihres gesamten Netzwerkes führen!

Kontrollieren Sie die Firmwareversion die Sie aufspielen möchten, auf Kompatibilität mit Ihrem Wireless Access Point.

Lesen Sie unbedingt die Hinweise auf der Herstellerseite, von wo aus Sie die Firmwaredatei herunterladen.

Führen Sie das Update nur dann durch wenn genügend zeitlicher Spielraum zur Verfügung steht, damit ein evtl. Problemfall gelöst werden kann, ohne dass die damit verbundene Ausfallzeit weitergehende Schäden verursacht

Notwendige Maßnahmen zum Schutz Ihres Netzwerkes

Treffen Sie folgende Maßnahmen um Ihr Netzwerk vor unberechtigtem Zugriff zu schützen:

- Ändern Sie das vorgegebene Passwort der Wireless Access Point Software. Dieses schützt vor unberechtigtem Zugriff, wobei die Passwortlänge und die Zeichenkette eine entscheidende Rolle bei der Sicherheit darstellt. Je länger ein Passwort, je kryptischer (Passwort zusammen gesetzt aus nicht logisch aufeinander folgenden alphanumerischen Zeichen), desto schwerer der unberechtigte Zugriff.

- Aktivieren Sie das WPA Verschlüsselungssystem in der Wireless Access Point Software.

- Benutzen Sie die MAC-Filter Funktion, um Computern mit unbekannter MAC-Adresse den Zugriff auf das Netzwerk zu verweigern.

Weiterführende Informationen zum Thema Sicherheit in der Informationstechnik erhalten Sie auf der Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI): http://www.bsi.bund.de

Inhaltsverzeichnis

KAPITEL 1 EINLEITUNG 1

1.1 VERPACKUNGSINHALT 2

1.2 FEATURES 2

1.3 SPEZIFIKATIONEN 2

1.4 TECHNISCHE BESCHREIBUNG 3

KAPITEL 2 WIRELESS LAN ACCESS POINT ANSCHLUSS 6

KAPITEL 3 WIRELESS LAN ACCESS POINT KONFIGURATION..... 7

3.1 INBETRIEBNAHME 7

3.2 KONFIGURATION DES WIRELESS ACCESS POINTS 11

3.2.1 Status und Information 12

3.2.2 Wireless Einstellungen 12

3.2.3 Erweiterte Einstellungen 24

3.2.4 AP Sicherheit 26

3.2.5 MAC-Adressen-Filtering 35

3.2.6 Systemprogramm 37

3.2.7 Configuration Tool 41

3.2.8 Firmware Upgrade 43

3.2.9 Reset 44

KAPITEL 4 GLOSSAR 45

Kapitel 1 Einleitung

WAP-0006/0009 ist ein Wireless Access Point für den Einsatz in einem IEEE 802.11g/b 2.4GHz kabellosen Netzwerk. Benutzer können diesen Wireless Access Point zum Aufbau eines WLANs verwenden. Mithilfe des „Infrastruktur Modus“ kann jede kabellose LAN-Station in ein WLAN eingebunden werden.

Das Produkt unterstützt WEP, WPA, ESSID und MAC-Adressen- Filter-Funktionen, um die Sicherheit des kabellosen Netzwerks zu festigen. Mittels ESSID-Authentifizierung, 64/128-Bit WEP-Verschlüsselung und MAC- Adressenfilterung wird verhindert, dass nicht autorisierte kabellose Stationen Zugriff auf das kabellose Netzwerk des Benutzers erhalten.

Die Dipolantenne des Wireless Access Points ist abnehmbar. Benutzer können am RP-SMA Anschluss des Wireless Access Points eine Hochleistungsantenne installieren, um die Qualität der Netzwerkverbindung zu verbessern. Dadurch wird eine höhere Flexibilität des kabellosen Netzwerks erreicht.
Dieses Produkt bietet eine einfach zu bedienende Benutzerschnittstelle und ermöglicht Benutzern die Konfiguration über den Web-Browser. Es enthält einen integrierten DHCP-Server, um mehreren kabellosen und verkabelten Benutzern ihre IP-Adresse automatisch zur Verfügung zu stellen.Wegen seiner vielseitigen Features, ist dieses Produkt die beste Wahl zur nahtlosen Integration von kabellosen und verkabelten Netzwerken.

1.1 Verpackungsinhalt

- WAP-0006/0009
- Stromadapter (nur WAP-0006)
- Programm-CD mit Handbuch
- Schnellinstallationsanleitung

1.2 Features

- Kompatibel mit IEEE 802.11b/g (DSSS) 2.4GHz Spezifikation.
- Entspricht IEEE 802.3af POE PD (Power Device) Standard (nur WAP-0009)
- 54Mbps Datenübertragungsrate.
- Nahtlose Integration von kabellosen und verkabelten Ethernet LAN Netzwerken.
- Auto-Fallback für Hindernisse oder Störungen.
- 64/128-Bit WEP- und WPA-Datenverschlüsselungsfunktion zum Schutz von kabellosen Datenübertragungen.
- Eingebauter DHCP-Server unterstützt automatische IP-Adressen- zuteilung.
- Unterstützt Web-basierende Konfiguration.

1.3 Spezifikationen

- Standards: IEEE 802.11b/g (kabellos), IEEE 802.3 (Kabel)
- Datenübertragungsrate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps Auto- Fallback
- Sicherheitsverschlüsselung: 64/128-bit WEP/
  WPA(802.1x, TKIP)
  WPA2(AES)
- Frequenzband: 2.400~2.4835GHz (Industrial Scientific Medical Band)
- Modulation: CCK@11/5.5Mbps, DQPSK@2Mbps und DBPSK@1Mbps
- Funktechnik: Direct Sequence Spread Spectrum (DSSS)
- Antenne: Externe, abnehmbare Dipolantenne (mit RP-SMA Anschluss)
- Anschlüsse: 10/100Mbps RJ-45 x 1
- Leistung: 12VDC, 0.5A
- Übertragungsleistung: 15dBm
- LEDs: Strom, LAN-Verbindung/Aktivität, Kabellose Aktivität
- Abmessungen: 30(H) x 127(B) x 96(T) mm

- Temperatur:
  Betrieb: 32~131°F (0~55°C)
  Lagerung: -4~158°F(-20~70°C)
- Feuchtigkeit: 10-90% (nicht-kondensierend)
- Zertifizierung: FCC, CE

1.4 Technische Beschreibung

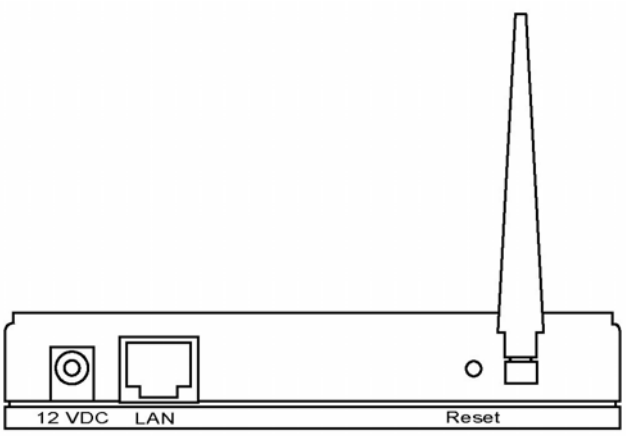
Frontblende

An der Frontblende des Wireless Access Points befinden sich LED-Anzeigen, die den Benutzer über den aktuellen Status des Geräts informieren. Nachfolgend ist eine Erklärung für jede LED.

LED	Farbe	Status	Bedeutung
Power	Grün	Leuchtet	Strom wird eingespeist.
		Aus	Kein Strom
WLAN	Grün	Blinkt	Antenne sendet oder empfängt Daten
		Aus	Antenne sendet oder empfängt keine Daten.
LAN	Grün	Ein	Eine gültige Verbindung ist hergestellt
		Blinkt	Daten werden gesendet oder empfangen.
		Aus	Keine Verbindung hergestellt.

Rückseite

Die Anschlussports des Wireless Access Points befinden sich an der Rückseite. Nachfolgend ist eine Erklärung für jeden Anschluss.



- Antennenanschluss
  Dieser runde Anschluss ist ein Standard-Reverse-SMA-Anschluss. Jede Antenne mit einem Reverse-SMA-Stecker kann mit dem Wireless Access Point verbunden werden.

- DC Adapteranschluss
  Verbinden Sie den Stecker des Stromadapters mit diesem Anschluss.

- LAN-Anschluss
  An den LAN-Anschluss des Wireless Access Points kann ein weiteres Netzwerkgerät angeschlossen werden.

- Reset
  Der Reset-Knopf ermöglicht eine der zwei folgenden Optionen.

  1) Falls Probleme mit dem Wireless Access Point auftreten, halten Sie den Reset-Knopf mit einer Stiftspitze gedrückt (für weniger als 4 Sekunden). Der Wireless Access Point startet selbständig neu und behält die Originalkonfiguration des Benutzers bei.
  2) Falls die Probleme bestehen bleiben, noch größere Probleme auftreten oder Sie möglicherweise das Passwort vergessen haben, halten Sie den Reset-Knopf für länger als 4 Sekunden gedrückt, und der Wireless Access Point wird auf die

werksseitigen Standardeinstellungen zurückgesetzt (Warnung: Originalkonfiguration des Benutzers wird dabei durch die werksseitigen Einstellungen ersetzt).

Kapitel 2 Wireless LAN Access Point Anschluss

1. **Optimalen Standort für den WLAN Access Point finden.**
   Der beste Standort für den Wireless Access Point ist üblicherweise in der Mitte des kabellosen Netzwerks, in Blickrichtung zu allen mobilen Stationen.

2. **Anschließen des WAN Access Points an Router, Hub oder Switch.**
   Schließen Sie ein Ende eines Standard-UTP-Kabels an den LAN-Anschluss des Wireless Access Points und das andere Kabelende an einen Router, einen Hub oder einen Switch an. Der Wireless Access Point wird dann mit dem verkabelten LAN-Netzwerk verbunden.

3. **Anschließen des DC Stromadapters an Stromanschluss des WLAN Access Points. (WAP-0006)**
   Verwenden Sie nur den mit dem Wireless Access Point mitgelieferten Stromadapter. Bei Benutzung eines anderen Adapters, kann es zur Beschädigung des Geräts kommen.

4. **Verbinden Sie den Wireless LAN Access Point mit ihrem POE Adapter, Router, Hub oder Switch. (nur WAP-0009)**

   Verbinden Sie ein Ende eines standard UTP Kabels mit dem LAN Port des Access Points und das andere Ende des Kabel mit einem POE Port am POE Switch, Router, POE Hub oder POE Adapter. Der Access Point wird sich einschalten und ein Wireless Netzwerk zur verfügung stehen.

Die Hardwareinstallation ist vollständig.

Kapitel 3 Wireless LAN Access Point Konfiguration

3.1 Inbetriebnahme

Dieser Wireless Access Point ist mit einem Web-basierenden Konfigurationshilfsprogramm ausgestattet, das dem Benutzer die Konfiguration sowohl von verkabelten als auch kabellosen Stationen ermöglicht. Folgen Sie den nachstehenden Anweisungen, um die Konfiguration durchzuführen.

Von verkabelter Station

1. Stellen Sie sicher, dass sich die verkabelte Station im selben Subnetz wie der Wireless Access Point befindet.
Die Standard IP-Adresse und Subnetzmaske des Wireless Access Point lautet:
Standard IP-Adresse: 192.168.2.1
Standard Subnetz: 255.255.255.0

Konfigurieren Sie Ihren PC im gleichen Subnetz, wie beim Wireless Access Point.

1a) Windows 98SE/ME

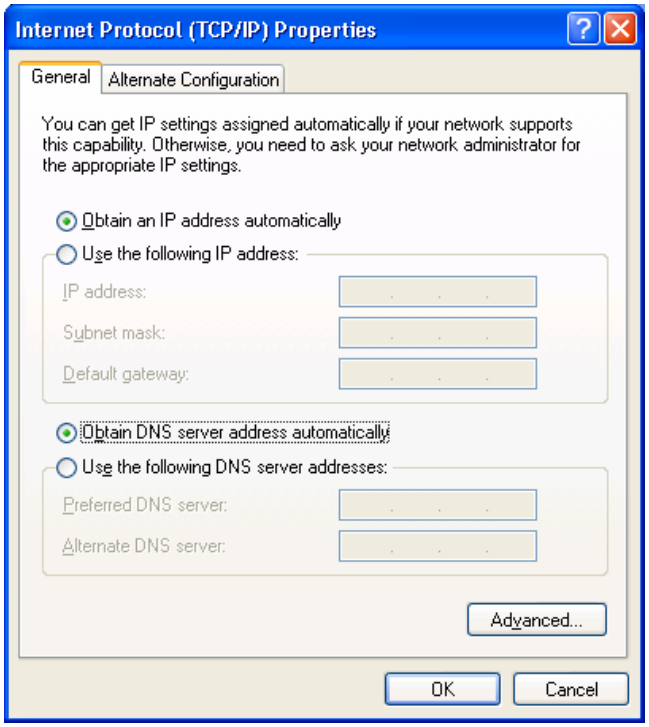
1. Klicken Sie die Schaltfläche *Start* und wählen *Einstellungen*; dann klicken Sie auf *Systemsteuerung*.
2. Doppelklicken Sie im Fenster *Systemsteuerung* das Symbol *Netzwerk*.
3. Prüfen Sie die Liste *Netzwerkkomponenten* im Fenster *Netzwerk*. Falls TCP/IP nicht installiert ist, klicken Sie die Schaltfläche *Hinzufügen*, um es jetzt zu installieren. Falls TCP/IP installiert ist, fahren Sie mit **Schritt 6** fort.
4. In der Dialogbox *Netzwerkkomponenten Typ* wählen Sie *Protokoll* und klicken die Schaltfläche *Hinzufügen*.
5. In der Dialogbox *Netzwerkprotokoll wählen*, wählen Sie *Microsoft und TCP/IP* und klicken dann die Schaltfläche *OK*, um das TCP/IP-Protokoll zu installieren. Zur Vervollständigung der Installation könnte Sie das System möglicherweise nach der Windows-CD fragen.
6. Nach der Installation von TCP/IP, gehen Sie zurück zur Dialogbox *Netzwerk*. Wählen Sie *TCP/IP* aus der Liste *Netzwerkkomponenten* aus und klicken dann die Schaltfläche *Eigenschaften*.
7. Prüfen Sie jede Registerkarte und gleichen die folgenden Einstellungen an:

- **Bindings**: Setzen Sie einen Haken in *Client für Microsoft Netzwerke* und *Datei- und Druckerfreigabe für Microsoft Netzwerke*.
- **Gateway**: Alle Felder bleiben leer.
- **DNS Konfiguration**: Wählen Sie *DNS Deaktivieren.*
- **WINS Konfiguration**: Wählen Sie *WINS Auflösung Deaktivieren.*
- **IP-Adresse**: Wählen Sie *Folgende IP-Adresse verwenden.* Geben Sie die IP-Adresse und Subnetzmaske, wie in folgendem Beispiel, ein.
  - ✓ IP-Adresse: 192.168.2.3 (jede IP-Adresse von 192.168.2.2 bis 192.168.2.254 ist verfügbar; **wählen Sie nicht 192.168.2.1**)
  - ✓ Subnetzmaske: 255.255.255.0

8. Starten Sie den PC neu. Der PC hat jetzt die eingegebene IP-Adresse übernommen.

1b) Windows XP

1. Klicken Sie die Schaltfläche *Start* und wählen *Einstellungen*; dann klicken Sie auf *Netzwerk verbindungen.* Das Fenster *Netzwerkverbindungen* wird geöffnet.
2. Doppelklicken Sie das Symbol *LAN-Verbindung*. Das Fenster *LAN-Verbindung* wird geöffnet. Klicken Sie die Schaltfläche *Eigenschaften.*
3. Prüfen Sie die Liste der Netzwerkkomponenten. Wählen Sie *Internetprotokoll [TCP/IP]* und klicken die Schaltfläche *Eigenschaften*.
4. Im Fenster *Eigenschaften von Internetprotokoll (TCP/IP)* wählen Sie *IP-Adresse automatisch beziehen* und *DNS-Serveradresse automatisch beziehen*, wie im folgenden Bildschirm gezeigt.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

5: Klicken Sie auf *OK,* um die Einstellung zu bestätigen. Der PC wird jetzt automatisch eine IP-Adresse vom DHCP-Server des Breitband Routers beziehen

Hinweis: Bitte vergewissern Sie sich, dass der DHCP-Server des Breitband Routers der einzige verfügbare DHCP-Server im LAN ist.

Sobald der PC zur automatischen Beziehung einer IP-Adresse konfiguriert ist, fahren Sie mit Schritt 3 fort.

1c) Windows 2000

1. Klicken Sie die Schaltfläche *Start* und wählen *Einstellungen;* dann klicken Sie *Systemsteuerung*. Das Fenster *Systemsteuerung* wird geöffnet.
2. Doppelklicken Sie das Symbol *Netzwerkverbindungen*. Im Fenster *Netzwerkverbindungen* doppelklicken Sie das Symbol *LAN-Verbindung*. Das Fenster *LAN-Verbindung* wird geöffnet.
3. Klicken Sie die Schaltfläche *Eigenschaften*.
4. Prüfen Sie die Liste *Netzwerkkomponenten*. Wählen Sie *Internetprotokoll [TCP/IP]* und klicken auf die Schaltfläche *Eigenschaften*.
5. Im Fenster *Eigenschaften von Internetprotokoll [TCP/IP]* wählen Sie *Folgende IP-Adresse verwenden* and geben IP-Adresse und Subnetzmaske, wie folgt ein.
   - ✓ IP-Adresse: 192.168.2.3 (jede IP-Adresse von 192.168.2.2 bis 192.168.2.254 ist verfügbar; **wählen Sie nicht 192.168.2.1**)
   - ✓ Subnetzmaske: 255.255.255.0
6. Klicken Sie *OK,* um die Einstellung zu bestätigen. Der PC hat jetzt die eingegebene IP-Adresse übernommen.

2. Tragen Sie **192.168.2.1** in Ihrem Web-Browser ein, um in das Konfigurationshilfsprogramm des Wireless Access Points zu gelangen.

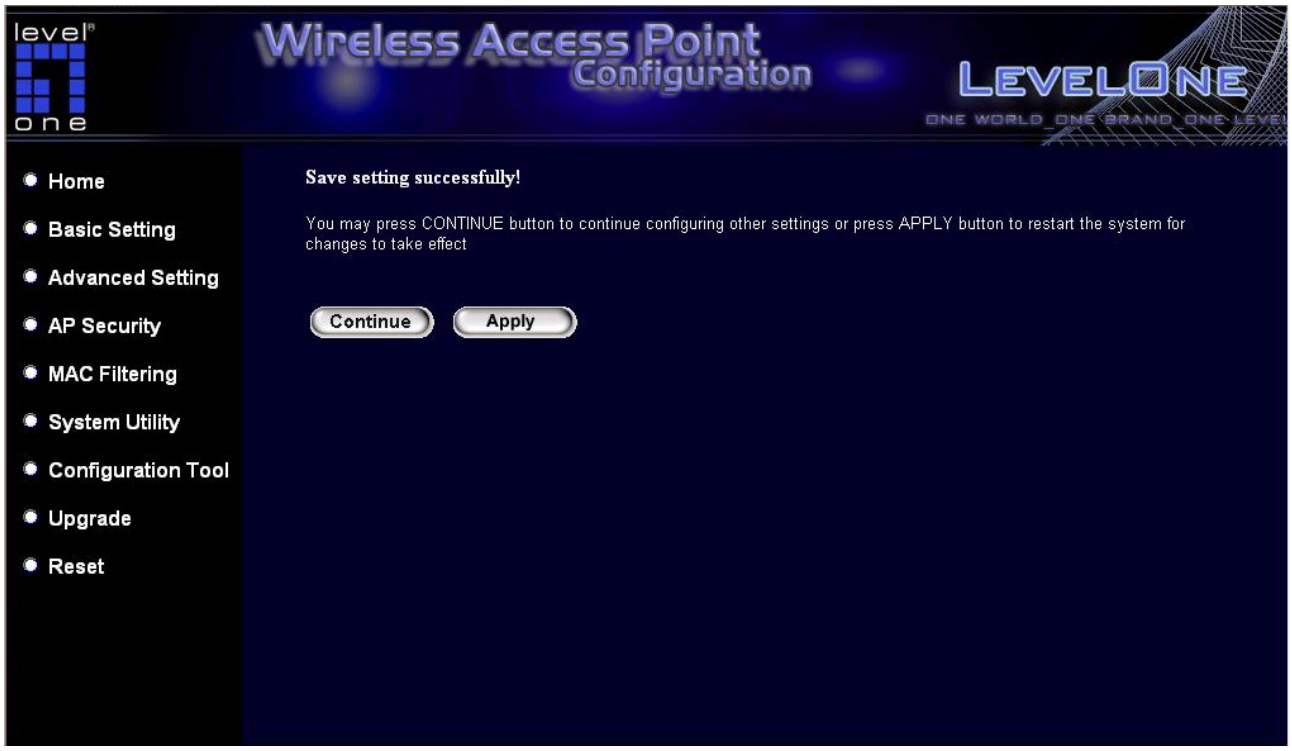
3. Ein Bildschirm erscheint und Sie werden zur Eingabe von Benutzername und Passwort aufgefordert. Standardname und –passwort sind wie folgt.
User Name: Admin
Password: 1234
Tragen Sie Standardname und –passwort ein und klicken auf **OK**.

4. Sie können mit der Konfiguration des Wireless Access Points beginnen.

Von kabelloser Station

1. Stellen Sie sicher, dass sich die kabellose Station im selben Subnetz wie der Wireless Access Point befindet. Bitte beziehen Sie sich zur Konfiguration der IP-Adresse und Subnetzmaske der kabellosen Station auf den obigen **Schritt 1**.
2. Zum Wireless Access Point verbinden:
   Die Standard-ESSID des Wireless Access Points lautet "**default**" und die WEP-Verschlüsselung ist deaktiviert. Stellen Sie sicher, dass die kabellose Station die gleiche ESSID benutzt wie der Wireless Access Point und verbinden die kabellose Station mit dem Wireless Access Point.
3. Tragen Sie **192.168.2.1** in Ihrem Web-Browser ein, um in das Konfigurationshilfs-programm des Wireless Access Points zu gelangen.
4. Tragen Sie Benutzername und Passwort ein und klicken auf **OK**. Der Wireless Access Point kann jetzt konfiguriert werden.

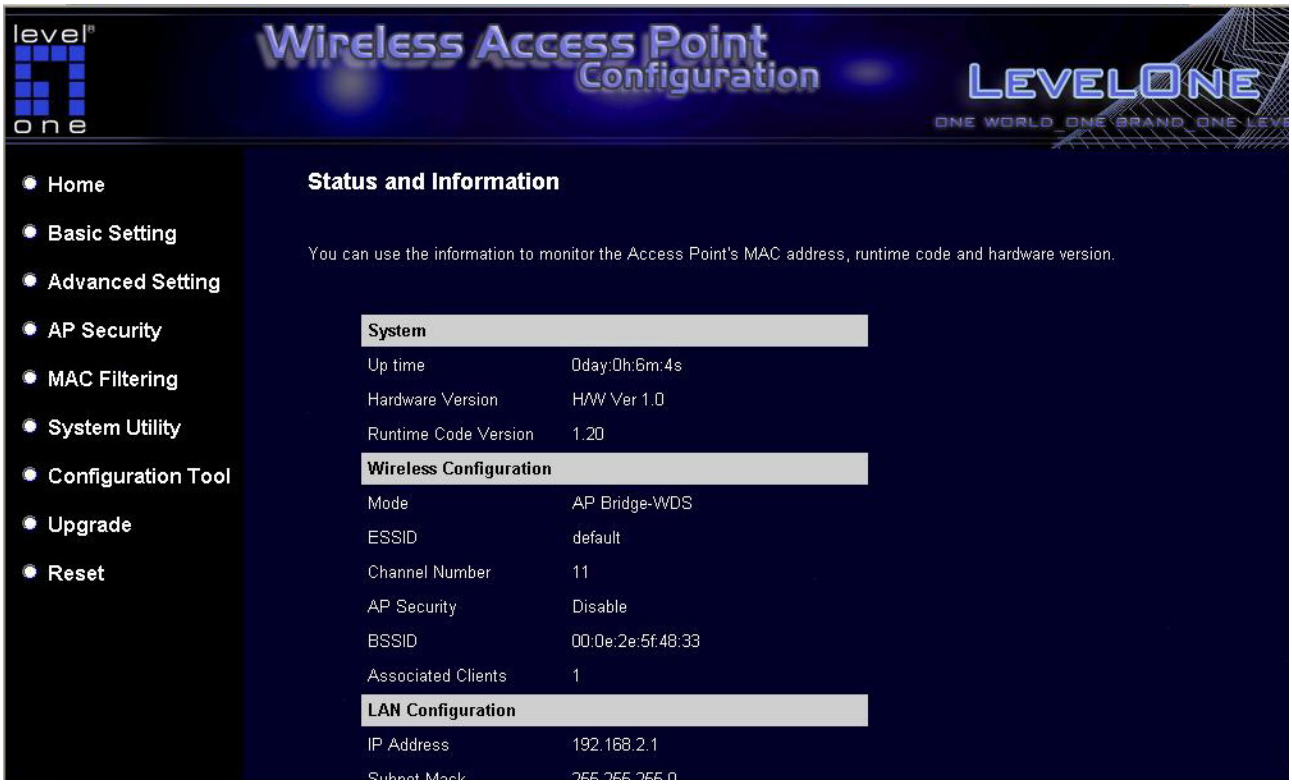
3.2 Konfiguration des Wireless Access Points



Jedes Mal, wenn durch den Benutzer Änderungen in einer Einstellungsseite vorgenommen werden und die Schaltfläche “APPLY” geklickt wird, öffnet sich die entsprechende Seite. Die Einstellungen werden erfolgreich gespeichert, aber treten nicht sofort in Kraft. Um die neuen Einstellungen wirksam zu machen, muss der Wireless Access Point neu gestartet werden. Durch Klicken der Schaltfläche “CONTINUE”, kann mit anderen Einstellungen fort gefahren werden. Die Schaltfläche “APPLY” kann auch gewählt werden, um das System neu zu starten und die Einstellungen wirksam zu machen.

3.2.1 Status und Information

In diesem Bildschirm sind allgemeine Informationen über den Wireless Access Point einzusehen, wie beispielsweise Firmwareversion, ESSID, Kanalnummer, Status, IP-Adresse, MAC- Adresse, etc.



3.2.2 Wireless Einstellungen

Dieser Wireless Access Point unterstützt AP, Station, Bridge, WDS und Universal Repeater Modi. Der “AP Mode” bietet eine reine Access Point Funktion. Der einfachste Weg ein kabelloses LAN aufzubauen, ist die Benutzung des “AP Mode”.

Der “Station Mode” wird verwendet, um ein verkabeltes Netzwerkgerät, mit kabellosen Kommunikationsfähigkeiten auszustatten. Sowohl Ad Hoc- als auch Infrastrukturmodus werden im “Station Mode” unterstützt. Mittels des “Station-Ad Hoc Mode” kann ein Netzwerkgerät, durch Peer-to-Peer Kommunikation, in ein WLAN eingebunden werden. Mit dem “AP-Client Mode” kann ein Netzwerkgerät, durch einen Wireless Access Point, in ein kabelloses LAN eingebunden werden.

Der “AP Bridge Mode” bietet die Funktion, zwei oder mehr verkabelte Ethernet-Netzwerke durch ein WLAN zusammenzufügen. Zwei Access Points mit “AP Bridge-Point to Point Mode” werden gebraucht, um zwei verkabelte Ethernet-Netzwerke zusammenzufügen. Wenn mehr als zwei verkabelte Ethernet-Netzwerke zusammengefügt werden sollen, müssen genug Access Points mit “AP Bridge-Point to Multi-Point Mode” zur Verfügung stehen.

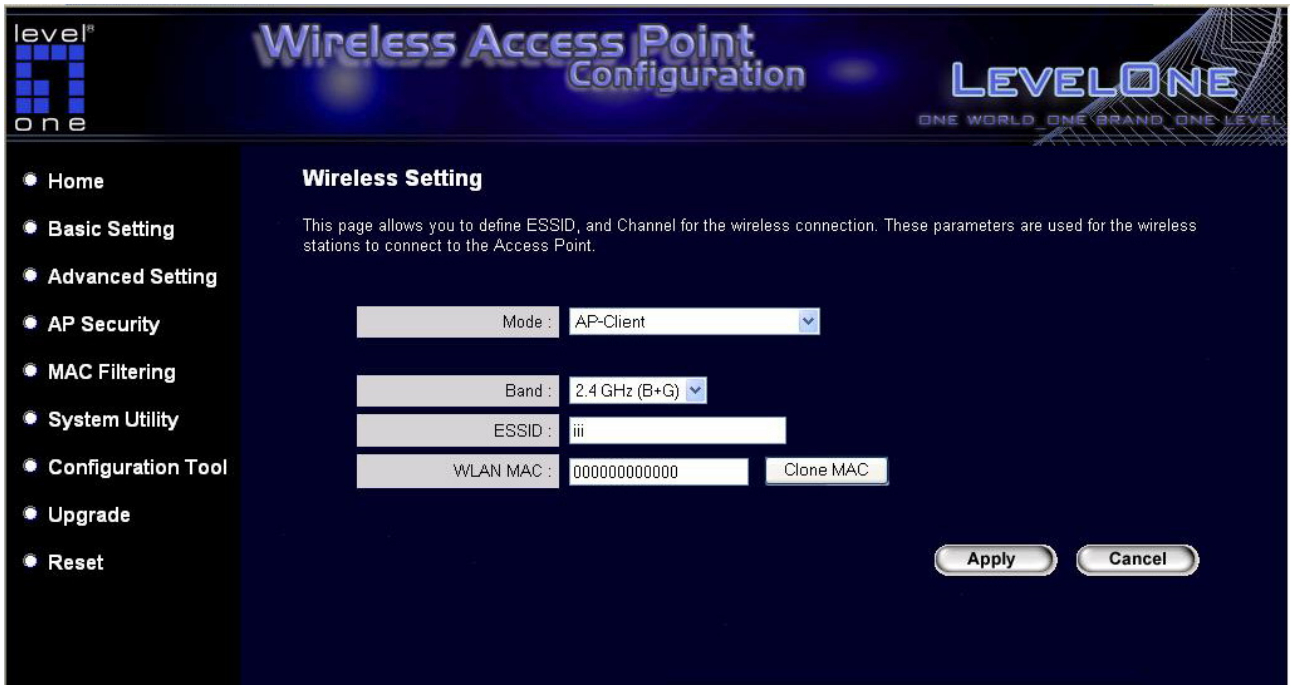
Ein Access Point mit “AP Bridge-Point to Point Mode” oder “AP Bridge-Point to Multi-Point Mode” kann nur zum Zusammenfügen von verkabelten Ethernet-Netzwerken benutzt werden. Eine zeitgleiche Verbindung von einer anderen kabellosen Station wird nicht akzeptiert. Wenn ein Access Point zum Zusammenfügen von verkabelten Ethernet-Netzwerken gebraucht wird und gleichzeitig Verbindung zu einer anderen kabellosen Station herstellen soll, muss der Access Point umgestellt werden auf “AP Bridge-WDS Mode”.

Einfach ausgedrückt ist die “AP Bridge-WDS Mode” Funktion eine Kombination aus “AP Mode” und “AP Bridge-Point to Multi-Point Mode”. “Universal Repeater Mode” bietet die Funktion gleichzeitig als Access Point Client und Access Point zu arbeiten. Der Modus benutzt die Access Point Client-Funktion, um zu einem Root Access Point zu verbinden und die Access Point Funktion, um alle kabellosen Stationen innerhalb der Reichweite zu versorgen. Alle Stationen innerhalb der Reichweite des Access Points können zum Root Access Point geschaltet werden. “Universal Repeater Mode” ist sehr geeignet, um die Reichweite des kabellosen Netzwerks zu erweitern.

Access Point-Modus Einstellungsseite:

Station-Ad Hoc-Modus Einstellungsseite:

AP-Client-Modus Einstellungsseite:



Access Point Bridge-Point to Point-Modus Einstellungsseite:

Wireless Access Point Configuration
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Home
Basic Setting
Advanced Setting
MAC Filtering
System Utility
Configuration Tool
Upgrade
Reset
Wireless Setting
This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.
Mode : AP Bridge-Point to Point
Band : 2.4 GHz (B+G)
Channel Number : 11
MAC Address 1 : 000000000000
Set Security : Set Security
Apply
Cancel

Access Point Bridge-Point to Multi-Point-Modus Einstellungsseite:

Wireless Access Point Configuration
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Home
Basic Setting
Advanced Setting
MAC Filtering
System Utility
Configuration Tool
Upgrade
Reset
Wireless Setting
This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.
Mode : AP Bridge-Point to Multi-Point
Band : 2.4 GHz (B+G)
Channel Number : 11
MAC Address 1 : 000000000000
MAC Address 2 : 000000000000
MAC Address 3 : 000000000000
MAC Address 4 : 000000000000
MAC Address 5 : 000000000000
MAC Address 6 : 000000000000
Set Security : Set Security

Access Point Bridge-WDS-Modus Einstellungsseite:

Wireless Access Point Configuration
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Home
Basic Setting
Advanced Setting
AP Security
MAC Filtering
System Utility
Configuration Tool
Upgrade
Reset
Wireless Setting
This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.
Mode : AP Bridge-WDS
Band : 2.4 GHz (B+G)
ESSID : default
Channel Number : 11
Associated Clients : Show Active Clients
MAC Address 1 : 000000000000
MAC Address 2 : 000000000000
MAC Address 3 : 000000000000
MAC Address 4 : 000000000000
MAC Address 5 : 000000000000
MAC Address 6 : 000000000000

Universal Repeater-Modus Einstellungsseite:

Parameter	Bedeutung
ESSID	Die ESSID (bis zu 31 druckfähige ASCII-Zeichen) ist der eindeutig zu identifizierende Name in einem WLAN. Die ID verhindert das unbeabsichtigte Verbinden von zwei geografisch nebeneinander agierenden WLANs. Vergewissern Sie sich, dass die ESSID von allen Stationen im gleichen WLAN identisch ist. Die Standard-ESSID ist “**default**”. Die ESSID muss im “AP Mode”, “Station-Ad Hoc Mode”, “AP-Client Mode”, “AP Bridge-WDS Mode” und “Universal Repeater Mode” vom Benutzer zugeteilt werden.
Band	Ermöglicht die Einstellung des AP für 802.11b oder 802.11g Modus. Auch der B+G Modus kann eingestellt werden, damit der AP automatisch zwischen 802.11b und 802.11g Verbindungen auswählen kann.
Channel Number	Wählen Sie zur Übereinstimmung mit den Netzwerkeinstellungen, den passenden Kanal aus der Liste aus. Die Kanäle unterscheiden sich von Land zu Land. Kanal 1-11 (Nordamerika) Kanal 1-14 (Japan) Kanal 1-13 (Europa) Es gibt 14 verfügbare Kanäle.

	Die Kanalnummer muss im “AP Mode”, “Station-Ad Hoc Mode”, “AP Bridge-Point to Point Mode”, “AP Bridge-Point to Multi-Point Mode”, “AP Bridge-WDS Mode” und “Universal Repeater Mode” vom Benutzer zugewiesen werden.
MAC Address	Wenn mehr als ein verkabeltes Ethernet-Netzwerk mit einem WLAN zusammengefügt werden soll, muss dieser AP auf “AP Bridge-Point to Point Mode”, “AP Bridge-Point to Multi-Point Mode” oder “AP Bridge-WDS Mode” eingestellt werden. Die MAC-Adressen von anderen Access Points in diesem Gefüge müssen vom Benutzer zugeteilt werden.
WLAN MAC	Im “Station-Ad Hoc Mode”, “AP-Client Mode” und “Universal Repeater Mode” benötigt dieses Gerät eine WLAN MAC-Adresse, um wie eine Station arbeiten zu können und zu anderen Netzwerkendpunkten (Peers) oder Access Points zu verbinden. Um dieses Gerät zu konfigurieren, können Sie auch die Schaltfläche “Clone MAC” klicken, damit der AP die MAC-Adressen kopiert, die der PC benutzt.
Root AP SSID	Im “Universal Repeater Mode” arbeitet dieses Gerät wie eine Station, um zu einem Root AP zu verbinden. Hier muss die SSID des Root APs vom Benutzer eingetragen werden. **Anmerkung: "AP Security" füt Universal Repeater Verschlüsselung benutzen**
Set Security	Klicken Sie im “AP Bridge-Point to Point Mode”, “AP Bridge-Point to Multi-Point Mode” und “AP Bridge-WDS Mode” auf “Set Security”, um eine Verschlüsselung für die Kommunikation zwischen zusammengefügten APs zu aktivieren. Dies schützt Ihr kabelloses Netzwerk. **Anmerkung: "Set Security" klicken, wenn "AP Bridge-WDS Mode" als Bridge Verschlüsselung benutzt wird, für WDS AP Verschlüsselung "AP Security" für Verschlüsselungseinstellung benutzen.**
Associated Clients	Klicken Sie die Schaltfläche “Show Active Clients”. Es öffnet sich die Tabelle “Active Wireless Client Table”. Hier können Sie den Status aller, mit diesem AP verbundenen, aktiven kabellosen Stationen sehen.
Wireless Site Survey	Wenn Sie den AP als kabellose Station für ein verkabeltes Netzwerkgerät einsetzen, müssen Sie ihn mit einem aktiven AP verbinden. Klicken Sie die Schaltfläche “Select Site Survey” und die Tabelle “Wireless Site Survey Table” wird geöffnet. Alle nahe gelegenen verfügbaren APs werden aufgelistet und Sie können einen AP auswählen. Er wird dann durch diesen AP in das WLAN eingebunden.

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt die Erweiterten Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

Set AP Security

Mit “Set Security” richten Sie die Sicherheit für die kabellose Datenüber-tragung zwischen den zusammengefügten Access Points im “AP Bridge-Point to Point Mode”, “AP Bridge-Point to Multi-Point Mode” oder “AP Bridge-WDS Mode” ein. Es stehen die Verschlüsselungsstandards “WEP 64bits”, “WEP 128bits”, “WPA (TKIP)” und “WPA2 (AES)” zur Verfügung.

WDS Security Settings
This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.
Encryption :
None
WEP Key Format :
ASCII
WEP Key :
Pre-Shared Key Format :
Passphrase
Pre-Shared Key :
Apply
Cancel

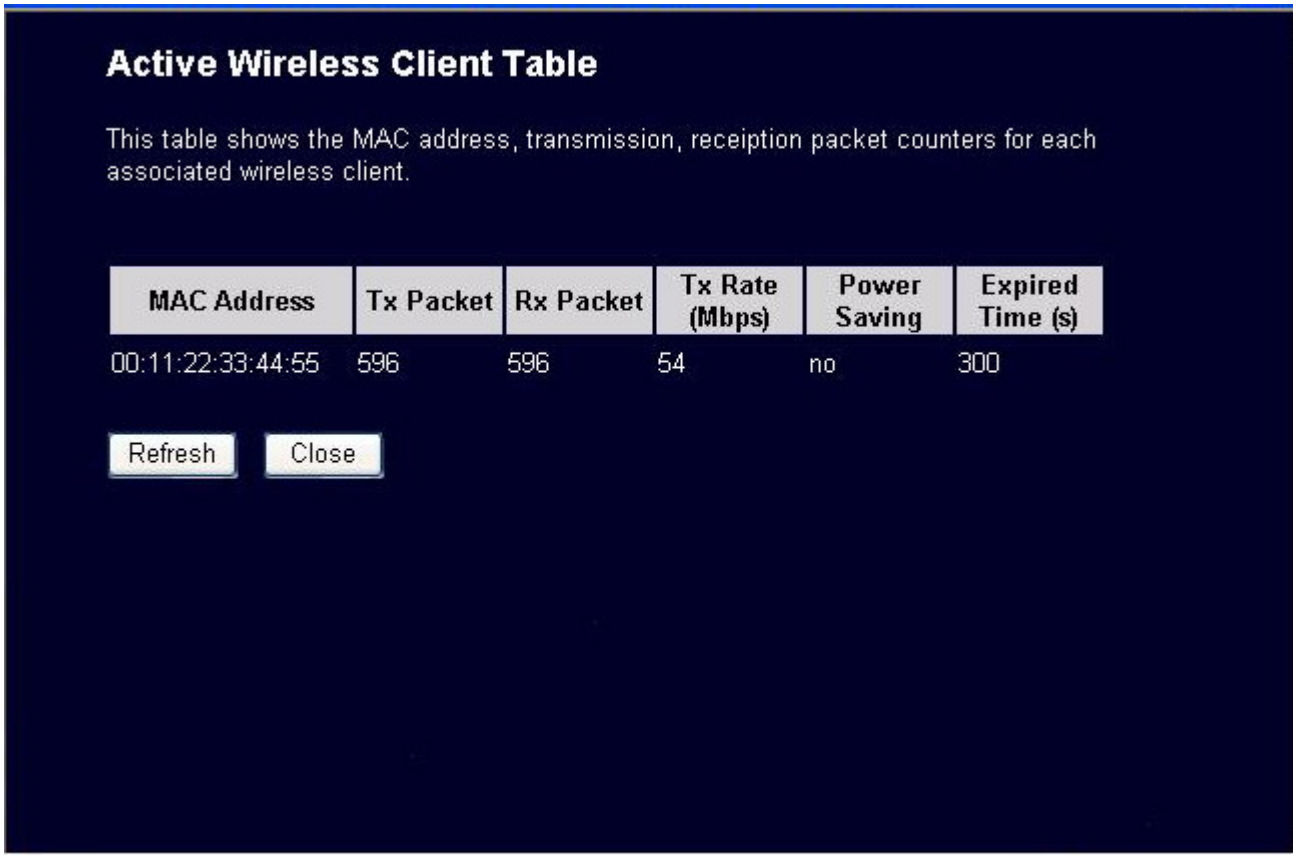
Parameter	Bedeutung
Encryption	Sie können auswählen zwischen “No encryption”, “WEP 64bits”, “WEP 128bits”, “WPA (TKIP)” oder “WPA2 (AES)” als Verschlüsselungs-standard.
Key Format	Wird nur gebraucht, wenn Sie ”WEP 64bits” oder “WEP 128bits” als Standard auswählen. Verwenden Sie ASCII-Zeichen (alphanumerisches

	Format) oder Hexadezimale Ziffern (von “A-F”, “a-f” und “0-9”) als WEP-Schlüssel, wie im folgenden Beispiel: ASCII-Zeichen: gast1 Hexadezimale Ziffern: 12345abcde
WEP Key	Wird nur gebraucht, wenn Sie “WEP 64bits” oder “WEP 128bits” als Standard auswählen. Der WEP-Schlüssel verschlüsselt die, zwischen den zusammengefügten APs, übertragenen Daten. Nehmen Sie Eintragungen in das Textfeld nach folgenden Regeln vor: 64-bit WEP: 10-stellige Hexwerte (von “A-F”, “a-f” und “0-9”) oder 5-stellige ASCII-Zeichen als Schlüssel. 128-bit WEP: 26-stellige Hexwerte (von “A-F”, “a-f” und “0-9”) oder 10-stellige ASCII-Zeichen als Schlüssel.
Pre-shared Key Format	Sie können zwischen Passphrase (alphanumerisches Format) oder Hexadezimalen Ziffern (von “A-F”, “a-f” und “0-9”) als Pre-Shared-Schlüssel auswählen, wie im folgenden Beispiel: Passphrase: ichbingast Hexadezimale Ziffern: 12345abcde
Pre-shared Key	Der Pre-Shared-Schlüssel dient der Authentifizierung und Verschlüsselung von Daten, die zwischen den zusammengefügten APs übertragen werden. Nehmen Sie Eintragungen in das Textfeld nach folgenden Regeln vor: 64-stellige Hexwerte (von “A-F”, “a-f” und “0-9”) oder mindestens 8-stellige Passphrase als Pre-Shared-Schlüssel.

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt die Erweiterten Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

Active Wireless Client Table

In der Tabelle “Active Wireless Client Table” wird der Status aller aktiven kabellosen Stationen protokolliert, die mit dem Wireless Access Point verbunden sind. Diese Tabelle zeigt die MAC-Adresse, die Anzahl der gesendeten und übertragenen Datenpakete und den Verschlüsselungsstatus jedes aktiven, kabellosen Clients an.

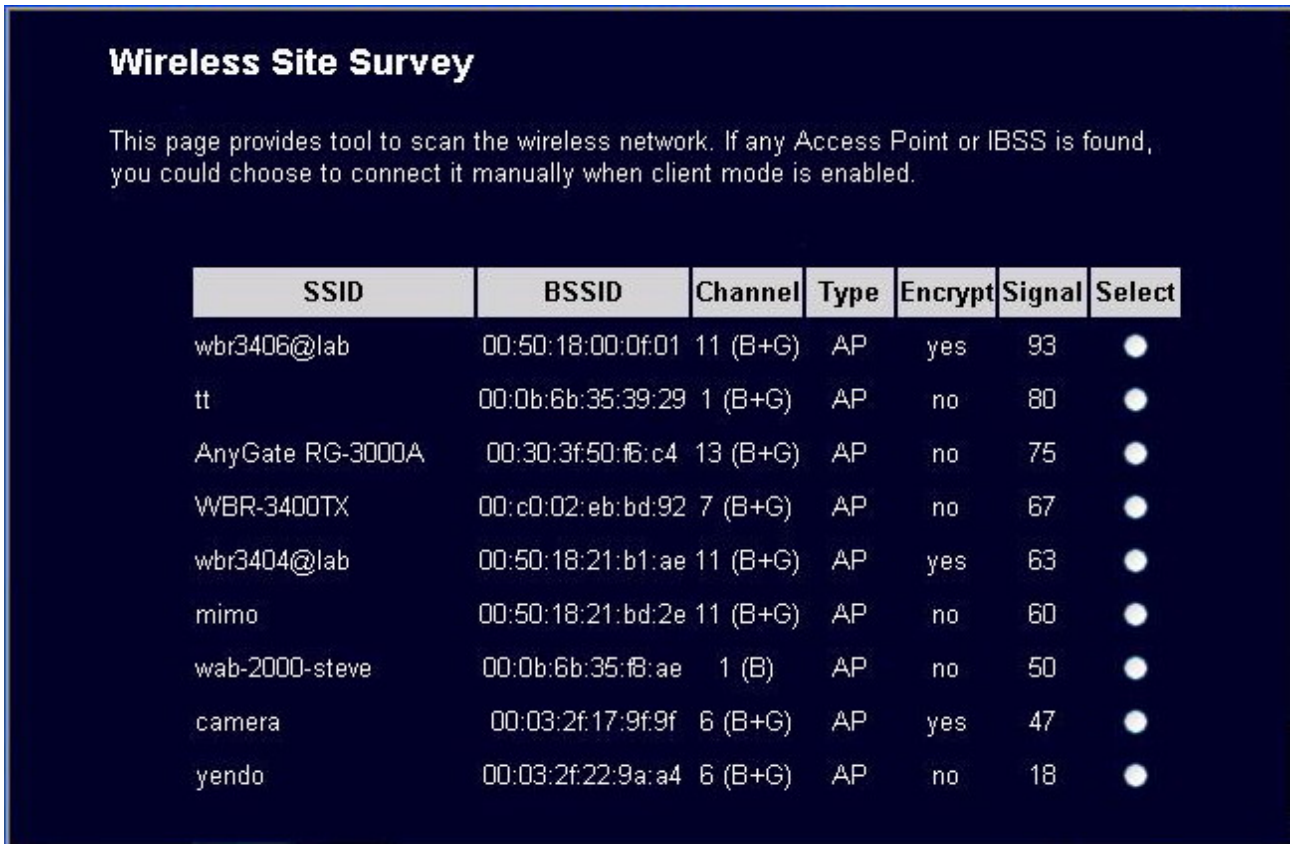


Parameter	Bedeutung
MAC Address	MAC-Adresse der aktiven kabellosen Station.
Tx Packet	Die Anzahl der Datenpakete, die von der aktiven kabellosen Station gesendet wurden.
Rx Packet	Die Anzahl der Datenpakete, die von der aktiven kabellosen Station empfangen wurden.
TX Rate	Die Übertragungsrate in Mbps.

Power Saving	Zeigt an, ob sich der kabellose Client im Energiesparmodus befindet.
Expired Time	Zeit, in Sekunden, vor der Trennung. Wenn die Leerlaufzeit des kabellosen Clients länger anhält als die Expired Time (Ablaufzeit), trennt dieser AP die Verbindung zum Client. Die Client-Station muss sich dann bei Aktivität erneut verbinden.
Refresh	Aktualisiert die Tabelle “Active Wireless Client Table”.
Close	Schließt die Tabelle “Active Wireless Client Table”.

Wireless Site Survey

Wenn sich dieser Wireless Access Point im “Station-Ad Hoc Mode”, “AP-Client Mode” oder im “Universal Repeater Mode” befindet, verbindet er sich mit einem anderen Access Point oder einer Station. Durch diesen verknüpften Access Point (oder Station) verbindet er dann zum WLAN. “Wireless Site Survey” sucht nach allen nah gelegenen Access Points. Sie können einen Access Point auswählen, der in dieser Tabelle aufgelistet ist.


Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
SSID BSSID Channel Type Encrypt Signal Select
wbr3406@lab 00:50:18:00:0f:01 11 (B+G) AP yes 93
tt 00:0b:6b:35:39:29 1 (B+G) AP no 80
AnyGate RG-3000A 00:30:3f:50:f6:c4 13 (B+G) AP no 75
WBR-3400TX 00:c0:02:eb:bd:92 7 (B+G) AP no 67
wbr3404@lab 00:50:18:21:b1:ae 11 (B+G) AP yes 63
mimo 00:50:18:21:bd:2e 11 (B+G) AP no 60
wab-2000-steve 00:0b:6b:35:f8:ae 1 (B) AP no 50
camera 00:03:2f:17:9f:9f 6 (B+G) AP yes 47
yendo 00:03:2f:22:9a:a4 6 (B+G) AP no 18

3.2.3 Erweiterte Einstellungen

Sie können auch erweiterte Parameter für diesen Wireless Access Point einrichten. Die Parameter umfassen Authentifizierungstyp, Fragmentierungsschwelle, RTS- Schwelle, Leitstrahl-Intervall, Tx Betriebsrate, Tx Basisrate, Präambel- typ, und Broadcast-ESSID. Änderungen dieser Parameter werden aber nur erfahrenen Benutzern empfohlen.

Wireless Access Point Configuration
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Home
Basic Setting
Advanced Setting
AP Security
MAC Filtering
System Utility
Configuration Tool
Upgrade
Reset
Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.
Authentication Type : Open System Shared Key Auto
Fragment Threshold : 2346 (256-2346)
RTS Threshold : 2347 (0-2347)
Beacon Interval : 100 (20-1024 ms)
Data Rate : Auto
Preamble Type : Long Preamble Short Preamble
Broadcast ESSID : Enabled Disabled
IAPP : Enabled Disabled
802.11g Protection : Enabled Disabled
Apply
Cancel

Parameter	Bedeutung
Authentication Type	Es gibt zwei Authentifizierungstypen: “Open System” and “Shared Key”. Wenn Sie “Open System” wählen, können sich kabellose Stationen mit diesem AP ohne WEP-Verschlüsselung verbinden. Wenn Sie “Shared Key” wählen, sollten Sie ebenso den WEP-Schlüssel auf der Seite “Encryption” einrichten. Kabellose Stationen sollten während der Authentifizierung WEP-Verschlüsselung benutzen, um mit diesem AP zu verbinden. Wenn Sie “Auto” wählen, kann der Client mit diesem Wireless Access Point verbinden, indem einer der beiden Authentifizierungstypen benutzt wird.
Fragment Threshold	“Fragment Threshold” gibt die maximale Größe von zu übertragenden Datenpaketen während der Datenfragmentierung an. Ist der Schwellwert zu niedrig, kommt es zu einer schwächeren Leistung.

RTS Threshold	Wenn die Paketgröße kleiner ist als die RTS-Schwelle, benutzt der AP nicht den RTS/CTS-Mechanismus, um dieses Paket zu senden.
Beacon Interval	Das Zeitintervall, in dem dieser AP ein Beacon (Leitstrahl) sendet. Der Leitstrahl wird zur Synchronisation des kabellosen Netzwerks benötigt.
Data Rate	“Data Rate” ist die Rate, die dieser AP verwendet, um Datenpakete zu übertragen. Der AP benutzt die größtmögliche ausgewählte Rate, um die Datenpakete zu übertragen.
Preamble Type	Der Präambeltyp definiert die CRC-Blocklänge in den Frames während der kabellosen Kommunikation. “Short Preamble” ist für kabellose Netzwerke mit hohem Datenverkehr geeignet. “Long Preamble” bietet eine zuverlässigere Kommunikation.
Broadcast ESSID	Wenn Sie “Broadcast ESSID” aktivieren, kann jede kabellose Station, diesen AP, innerhalb seiner Reichweite, leicht erkennen. Wenn Sie ein öffentliches kabelloses Netzwerk aufbauen, ist die Aktivierung dieses Features empfohlen. Die Deaktivierung von “Broadcast ESSID” bietet eine höhere Sicherheit.
IAPP	Wenn Sie “IAPP” aktivieren, sendet der AP automatisch Informationen von verbundenen kabellosen Stationen zu seinen Nachbarn. Dadurch ist nahtloses Roaming von kabellosen Stationen zwischen APs möglich. Wenn sich mehr als ein AP im WLAN befindet, und die kabellosen Stationen über spezielle Roaminganforderungen verfügen, ist die Aktivierung dieses Features empfohlen. Die Deaktivierung von “IAPP” bietet eine höhere Sicherheit.
802.11g Protection	Dieses Feature ist zur Aktivierung des Schutzmechanismus empfohlen. Dieser Mechanismus vermindert die Kollision von Datenübertragungen zwischen 802.11b und 802.11g Stationen. Wenn der Schutzmodus aktiviert ist, verringert sich der Durchsatz des APs.

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt andere Erweiterte Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

3.2.4 AP Sicherheit

Dieser Wireless Access Point bietet alle WLAN Sicherheitsfunktionen, inkl. WEP, IEEE 802.1x, IEEE 802.1x mit WEP, WPA mit Pre-Shared Schlüssel und WPA mit RADIUS. Mit diesen Funktionen verhindern Sie unberechtigten Zugriff auf Ihr WLAN. Stellen Sie sicher, dass die kabellosen Stationen dieselbe Sicherheitsfunktion verwenden.

WEP

Wenn Sie einen 64-Bit oder128-Bit WEP-Schlüssel wählen, müssen Sie den WEP-Schlüssel eingeben, um Daten zu verschlüsseln. Sie können vier WEP-Schlüssel eingeben und einen davon als Standard-Schlüssel auswählen. Dann kann der Wireless Access Point alle Datenpakete empfangen, die von einem der vier Schlüssel verschlüsselt wurden. Sie können WEP-Verschlüsselung im “AP Mode”, “Station-Ad Hoc Mode”, “AP-Client Mode”, “AP Bridge-WDS Mode” und “Universal Repeater Mode” verwenden.

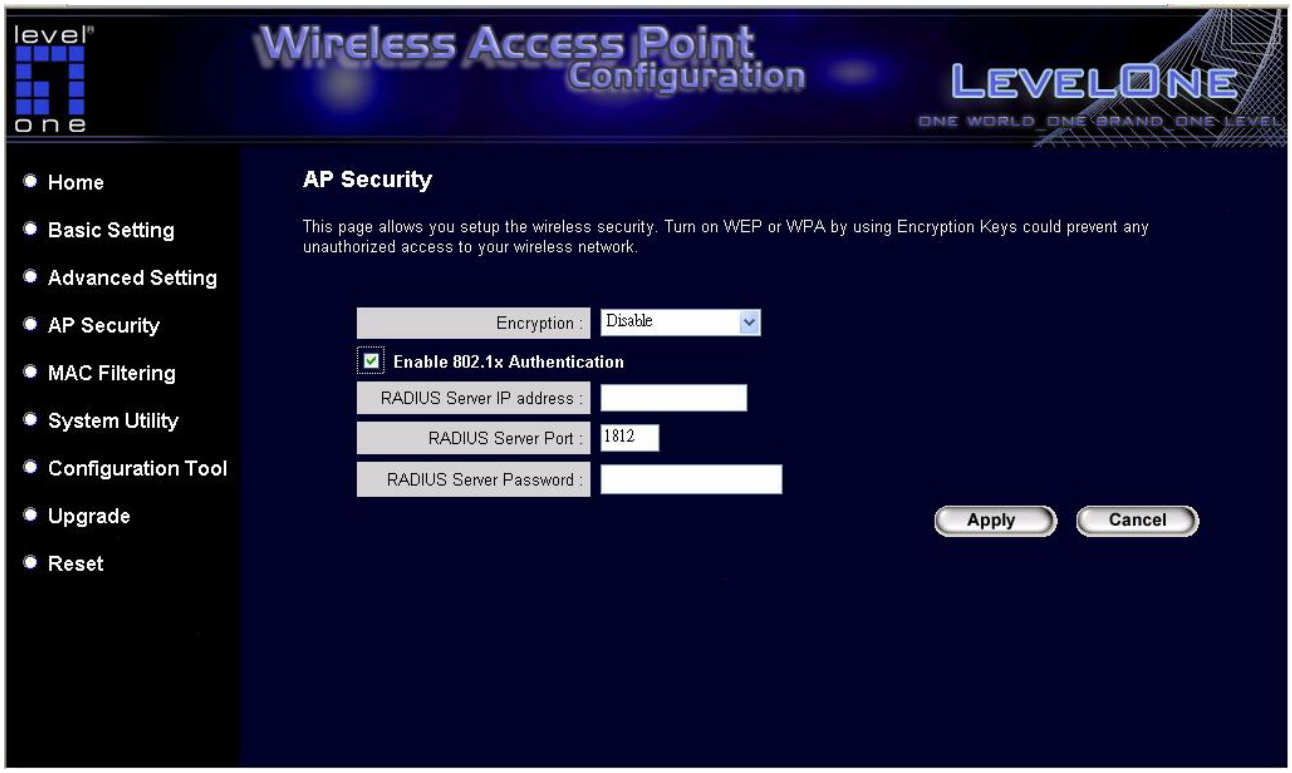
Parameter	Bedeutung
Key Length	Sie können den 64 oder 128-Bit Schlüssel zur Verschlüsselung übertragener Daten auswählen. Eine größere WEP-Schlüssellänge bietet eine höhere Sicherheit, aber der Durchsatz wird verringert.
Key Format	Verwenden Sie ASCII-Zeichen (alphanumerisches Format) oder Hexadezimale Ziffern (von “A-F”, “a-f” und “0-9”) als WEP-Schlüssel, wie im nachfolgenden Beispiel: ASCII-Zeichen: gast1 Hexadezimale Ziffern: 12345abcde
Default Tx Key	Wählen Sie einen der vier Schlüssel, um Daten zu verschlüsseln. Nur der Schlüssel, den Sie hier auswählen, ist wirksam.
Key 1 - Key 4	Die WEP-Schlüssel werden zur Verschlüsselung von übertragenen Daten im

	kabellosen Netzwerk benötigt. Nehmen Sie Eintragungen in das Textfeld nach folgenden Regeln vor. 64-bit WEP: 10-stellige Hexwerte (von “A-F”, “a-f” und “0-9”) oder 5-stellige ASCII-Zeichen als Schlüssel. 128-bit WEP: 26-stellige Hexwerte (von “A-F”, “a-f” und “0-9”) oder 10-stellige ASCII-Zeichen als Schlüssel

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt andere Erweiterte Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

802.1X

IEEE 802.1x ist ein Authentifizierungsprotokoll. Jeder Benutzer muss einen gültigen Account benutzen, um sich vor dem Zugriff auf das WLAN an diesem Wireless Access Point anzumelden. Die Authentifizierung wird von einem RADIUS-Server ausgeführt. Dieser Modus authentifiziert Benutzer nur durch IEEE 802.1x, aber verschlüsselt die Daten nicht während der Kommunikation. Sie können 802.1x ohne Verschlüsselung im “AP Mode”, “AP Bridge-WDS Mode” und “Universal Repeater Mode” verwenden.



Parameter	Bedeutung
RADIUS Server IP address	Die IP-Adresse des externen RADIUS-Servers.
RADIUS Server Port	Der Serveranschluss des externen RADIUS-Servers.
RADIUS Server Password	Das vom externen RADIUS-Server benutzte Passwort.

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt andere Erweiterte Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

802.1X WEP STATISCHER SCHLÜSSEL

IEEE 802.1x ist ein Authentifizierungsprotokoll. Jeder Benutzer muss einen gültigen Account benutzen, um sich vor dem Zugriff auf das WLAN an diesem Wireless Access Point anzumelden. Die Authentifizierung wird von einem RADIUS-Server ausgeführt. Dieser Modus verwendet auch WEP zur Verschlüsselung von Daten während der Kommunikation. Sie können 802.1x mit WEP-Verschlüsselung im “AP Mode”, “AP Bridge-WDS Mode” und “Universal Repeater Mode” verwenden.

Wireless Access Point Configuration
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Home
Basic Setting
Advanced Setting
AP Security
MAC Filtering
System Utility
Configuration Tool
Upgrade
Reset
AP Security
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Encryption : WEP
Key Length : 64-bit
Key Format : Hex (10 characters)
Default Tx Key : Key 1
Encryption Key 1 : **********
Encryption Key 2 : **********
Encryption Key 3 : **********
Encryption Key 4 : **********
Enable 802.1x Authentication
RADIUS Server IP address :
RADIUS Server Port : 1812
RADIUS Server Password :

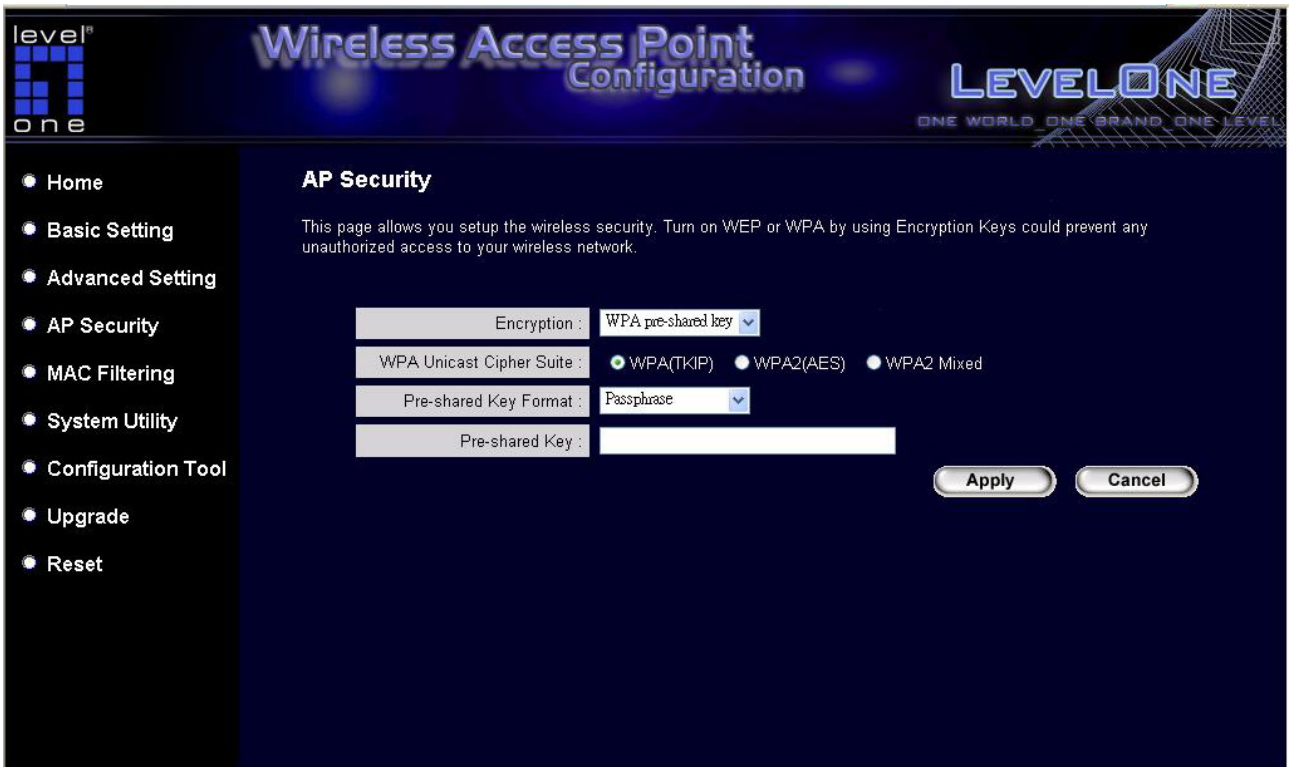
Für die WEP-Einstellungen, lesen Sie bitte den Abschnitt “WEP”. Für die 802.1x-Einstellungen, lesen Sie bitte den Abschnitt “802.1x”.

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt andere Erweiterte Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

WPA Pre-Shared Schlüssel

Wi-Fi Protected Access (WPA) ist ein erweiterter Sicherheitsstandard. Sie können einen Pre-Shared Schlüssel sowohl zur Authentifizierung von kabellosen Stationen als auch zur Datenverschlüsselung während der Kommunikation verwenden. Der Standard benutzt TKIP oder CCMP(AES), damit der Schlüssel aus Sicherheitsgründen regelmäßig geändert

wird und für Hacker nur schwer zu knacken ist. Die Verschlüsselung durch WPA Pre-Shared Schlüssel wird im “AP Mode”, “Station-Ad Hoc Mode”, “AP-Client Mode”, “AP Bridge-WDS Mode” und “Universal Repeater Mode” verwendet.



Parameter	Bedeutung
WPA (TKIP)	Der TKIP-Standard ändert regelmäßig den Schlüssel, um die Sicherheit im WLAN zu erhöhen.
WPA2 (AES)	Der AES-Standard erhöht ebenfalls die Sicherheit im WLAN. Das verwendete CCMP-Protokoll ändert dazu regelmäßig den Schlüssel.
WPA2 Mixed	TKIP oder AES werden, basierend auf dem anderen Netzwerkendpunkt (Peer), automatisch gewählt.
Pre-shared Key Format	Sie können zwischen Passphrase (alphanumerisches Format) oder Hexadezimalen Ziffern (von “A-F”, “a-f” und “0-9”) als Pre-Shared-Schlüssel auswählen, wie im folgenden Beispiel: Passphrase: ichbingast Hexadezimale Ziffern: 12345abcde:
Pre-shared Key	Der Pre-Shared-Schlüssel dient der Authentifizierung und Verschlüsselung von übertragenen Daten. Nehmen Sie Eintragungen in das Textfeld nach folgenden Regeln vor: 64-stellige Hexwerte (von “A-F”, “a-f” und “0-9”) oder mindestens 8-

stellige Passphrase als Pre-shared-Schlüssel

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt andere Erweiterte Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

WPA RADIUS

Wi-Fi Protected Access (WPA) ist ein erweiterter Sicherheitsstandard. Sie können einen externen RADIUS-Server sowohl zur Authentifizierung von kabellosen Stationen als auch zur Datenverschlüsselung während der Kommunikation verwenden. Der Standard benutzt TKIP oder CCMP(AES), damit der Schlüssel aus Sicherheitsgründen regelmäßig geändert wird und für Hacker nur schwer zu knacken ist. Die Verschlüsselung durch WPA RADIUS wird im “AP Mode”, “AP Bridge-WDS Mode” und “Universal Repeater Mode” verwendet.

Parameter	Bedeutung
WPA(TKIP)	Der TKIP-Standard ändert regelmäßig den Schlüssel, um die Sicherheit im WLAN zu erhöhen.
WPA2(AES)	Der AES-Standard erhöht ebenfalls die Sicherheit im WLAN. Das verwendete CCMP-Protokoll ändert dazu regelmäßig den Schlüssel.
WPA2 Mixed	TKIP oder AES werden, basierend auf dem anderen Endpunkt (Peer) des Netzwerks, automatisch gewählt.
RADIUS Server IP address	Die IP-Adresse des externen RADIUS-Servers.
RADIUS Server Port	Der Serveranschluss des externen RADIUS-Servers.
RADIUS Server Password	Das vom externen RADIUS-Server benutzte Passwort.

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt andere Erweiterte Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

3.2.5 MAC-Adressen-Filtering

Durch MAC-Adressen-Filtering wird verhindert, dass nicht autorisierte MAC-Adressen Zugriff auf das WLAN erhalten.

Parameter	Bedeutung
Enable Wireless Access Control	Aktivierung oder Deaktivierung der MAC-Adressen Filterfunktion.
MAC Address Filtering Table	In dieser Tabelle werden die MAC-Adressen der kabellosen Stationen protokolliert, denen der Zugriff auf das Netzwerk vom Benutzer gewährt wird. Im Feld “Comment” steht die Bezeichnung der kabellosen Station in Verbindung mit der MAC-Adresse (im Feld “MAC Address”). Diese Felder sind für den Benutzer hilfreich zur Erkennung der kabellosen Stationen.
Add MAC address into the table	Im Bereich “New” können Sie Adresse und Bezeichnung (“MAC Address” und “Comment”) einer neuen kabellosen Station eingeben. Klicken Sie anschließend auf “Add” und die kabellose Station wird in die Tabelle “MAC Address Filtering Table” hinzugefügt. Wenn Sie vor dem Hinzufügen einen Tippfehler bemerken, klicken Sie auf die Schaltfläche “Clear”. Die Eintragungen in den Feldern “MAC Address” und “Comment”

	werden gelöscht und sie können neue Eingaben vornehmen.
Remove MAC address from the table	Wenn Sie einige MAC-Adressen aus der Tabelle “MAC Address Filtering Table” entfernen möchten, wählen Sie die entsprechenden Adressen aus und klicken “Delete Selected”. Wenn Sie alle MAC-Adressen aus der Tabelle entfernen möchten, klicken Sie die Schaltfläche “Delete All”.
Reset	Wenn Sie auf die Schaltfläche “Reset” klicken, wird die aktuelle Auswahl aufgehoben.

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt andere Erweiterte Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

3.2.6 Systemprogramm

In diesem Menü können Sie die IP-Adresse des Wireless Access Points und das Login-Passwort definieren. Hier kann auch die DHCP-Serverfunktion des Wireless Access Points aktiviert werden.

Parameter	Bedeutung
Current Password	Geben Sie das aktuelle Passwort des Wireless Access Points ein (bis zu 15-stellige alphanumerische Zeichenkette). Das Standardpasswort für den Wireless Access Point lautet **1234**.
New Password	Geben Sie ein neues Passwort für die Anmeldung am Wireless Access Point ein (bis zu 15-stellige alphanumerische Zeichenkette).
Re-Enter Password	Bestätigen Sie das neue Passwort noch einmal.
IP Address	Bestimmen Sie die IP-Adresse des Wireless Access Points. Diese IP-Adresse muss einzigartig und eindeutig im Netzwerk sein. Die Standard IP-Adresse lautet **192.168.2.1**.
Subnet Mask	Bestimmen Sie eine Subnetzmaske für das LAN-Segment. Die Subnetz-maske des Wireless Access Point ist fest und lautet **255.255.255.0**.
Gateway Address	Die IP-Adresse des Standard-Gateways im Subnetz, in dem sich der

	Wireless Access Point befindet. Sie ermöglicht den Zugriff eines PCs auf den Wireless Access Point von einem anderen Subnetz zur Konfiguration.
DHCP Server	Aktivierung oder Deaktivierung des DHCP-Servers.

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt andere Erweiterte Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points beginnen.

DHCP Servereinstellungen

Der DHCP-Server vergibt automatisch eine IP-Adresse an den LAN-Client. Wenn DHCP nicht aktiviert ist, muss der Benutzer manuell eine IP-Adresse für den LAN-Client vergeben.

Parameter	Bedeutung
Default Gateway IP	Bestimmen Sie die Gateway-IP im Netzwerk. Diese IP-Adresse muss sich von der Management-IP unterscheiden.
Domain Name Server IP	Dies ist die IP-Adresse des DNS-Servers, die Sie von Ihrem ISP (Internet Service Provider) erhalten haben. Sie können auch Ihre eigene bevorzugte IP-Adresse für den DNS-Server bestimmen.
Start IP/End IP	Sie können einen bestimmten IP-Adressbereich für den DHCP-Server festlegen, um die IP-Adressen den LAN-Clients zuzuteilen. Der Standard IP-Bereich reicht von **192.168.2.100** bis **192.168.2.200**.
Domain Name	Sie können den Domänennamen für den Wireless Access Point festlegen.
Lease Time	Wenn der DHCP-Server aktiviert ist, erhält der LAN-Client vorübergehend eine IP-Adresse. In der Einstellung **Lease Time** bestimmen Sie die Dauer, für die der DHCP-Server dem LAN-Client eine IP-Adresse zur Verfügung stellt. Der DHCP-Server ändert die IP-Adresse, wenn diese Zeitspanne

abgelaufen ist.

Klicken Sie unten im Bildschirm auf die Schaltfläche **Apply**, um die oben stehenden Konfigurationen zu speichern. Sie können jetzt andere Erweiterte Einstellungen konfigurieren oder mit der Benutzung des Wireless Access Points.

3.2.7 Configuration Tool

Das Configuration Tool Menü ermöglicht dem Benutzer, über die Schaltfläche Backup, die Konfigurationseinstellungen des Wireless Access Points zu sichern. Die zuvor gesicherten Konfigurationseinstellungen können über die Schaltfläche Upload wiederhergestellt werden. Mit der Schaltfläche Browse kann eine zu ladende Konfiguration ausgewählt werden.

Mit der Schaltfläche Restore to Factory Default werden die Konfigurationseinstellungen auf die werksseitigen Standardeinstellungen zurückgesetzt. Dieses ist dann sinnvoll, wenn die zuvor getätigten Einstellungen einen Betrieb des Acces Points verhindern und die Konfiguration überprüft und neu eingestellt werden muss.

level one
Wireless Access Point
Configuration
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Home
Basic Setting
Advanced Setting
AP Security
MAC Filtering
System Utility
Configuration Tool
Upgrade
Reset
Configuration Tool
Use the "Backup" tool to save the Access Point's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Access Point. Alternatively, you can use the "Restore to Factory Default" tool to force the Access Point to perform System Reset and restore the original factory settings.
Backup Settings :
Save...
Restore Settings :
瀏覽...
Upload
Restore to Factory Default :
Reset

Parameter	Bedeutung
Configuration Tools	Mit der Schaltfläche **Backup** werden die Konfigurationseinstellungen des Wireless Wireless Access Points unter dem Namen config.bin. auf dem Computer, von wo aus die Benutzeroberfläche des Einstellungsprogramms gestartet wurde, gespeichert. Mit **Browse** können Sie die Konfigurationseinstellungen suchen und auswählen. Mit

	der Schaltfläche **Upload** werden sie auf den Wireless Wireless Access Point übertragen. Alternativ setzen Sie den Wireless Wireless Access Point, durch Klicken auf die Schaltfläche **Restore to Factory Default,** auf die Voreinstellungen zurück. Der Wireless Wireless Access Point wird nun heruntergefahren und erneut mit den Voreinstellungen

3.2.8 Firmware Upgrade

In diesem Menü können Sie eine neuere Firmwareversion für den Wireless Access Point einspielen

level one
Wireless Access Point Configuration
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Home
Basic Setting
Advanced Setting
AP Security
MAC Filtering
System Utility
Configuration Tool
Upgrade
Reset
WEB Upgrade
This tool allows you to upgrade the Access Point's system firmware.It is recommended that upgrading the firmware from wired stations.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.
瀏覽...
Apply
Cancel

Parameter	Bedeutung
Firmware Upgrade	Dieses Menü ermöglicht dem Benutzer eine neue oder andere Version der Firmware auf den Wireless Access Point aufzuspielen. Zu diesem Zweck laden Sie zuerst die Firmwaredatei auf den Computer, von dem Sie die Benutzeroberfläche des Einstellungsprogramms gestartet haben. Mit **Browse** können Sie die Firmwaredatei suchen und auswählen. Mit der Schaltfläche **Apply** wird sie auf den Wireless Access Point übertragen. Dieses kann einige Minuten dauern. Schalten Sie den Wireless Access Point in dieser Zeit nicht aus und lösen Sie keine Kabelverbindungen! Nach Fertigstellung ist ein Reset des Wireless Access Points durchzu-führen.

3.2.9 Reset

Bei Verbindungs- oder Funktionsproblemen kann der Wireless Access Point über dieses Menü neu gestartet werden.

level one
Wireless Access Point Configuration
LEVELONE
ONE WORLD ONE BRAND ONE LEVEL
Home
Basic Setting
Advanced Setting
AP Security
MAC Filtering
System Utility
Configuration Tool
Upgrade
Reset
Reset
In the event that the system stops responding correctly or stops functioning, you can perform a Reset. Your settings will not be changed. To perform the reset, click on the APPLY button below. You will be asked to confirm your decision. The Reset will be complete when the LED Power light stops blinking.
Apply
Cancel

Parameter	Bedeutung
Reset	In den Fällen, in denen es zu unvorhergesehenen Verbindungsabbrüchen oder Funktionsstörungen kommt, kann der Wireless Access Point neu gestartet werden. Hierbei werden die Konfigurationseinstellungen nicht verändert. Um den Wireless Access Point neu zu starten, klicken Sie auf die Schaltfläche **Apply.** Um den Neustart zu bestätigen, klicken Sie im folgenden Dialogfeld auf **OK**. Nachdem der Neustart durchgeführt wurde, kann der Wireless Acces Point mit den bisherigen Einstellungen benutzt werden.

Kapitel 4 Glossar

Account Mit dem Wort Account wird ein Benutzerkonto in der IT Umgebung bezeichnet. Dieses dient dem Zugang zu einem Computer, dem Internet, einem Netzwerk oder auch der Anmeldung bei Servern. Vor dem Zugriff muss man sich mit Benutzername und Passwort authentifizieren. Einem Benutzerkonto werden sehr oft Zugriffsrechte zugeordnet. Diese Rechte entscheiden über die Art des Zugriffs (Schreiben, Lesen, Ändern u.a.).

Ad-hoc Ein Ad-hoc-Netzwerk bezeichnet in der Informationstechnologie eine drahtlose Netzwerktopologie zwischen zwei oder mehr mobilen Endgeräten, die ohne feste Infrastruktur auskommt. Innerhalb des Netzes können mobile Geräte, wie z.B. Mobiltelefone, Kleincomputer oder Laptops, sofort eine Verbindung zueinander aufbauen, ohne dass eine übergeordnete Infrastruktur (wie z. B. Wireless Access Points) benötigt wird.

AES Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptosystem, welches als Nachfolger für DES bzw. 3DES im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekannt gegeben wurde.

ASCII-Zeichen (American Standard Code for Information Interchange) - Binärdatencode aus sieben Datenbits plus einem Bit für Parität oder spezielle Symbole; von ANSI definiert zur Kompatibilität zwischen Datendiensten.

Auto-Fallback Die Funktion des Fallbacks wird auch in WLANs nach 802.11a, 802.11b und 802.11g realisiert, wobei bei Unterschreiten einer bestimmten Empfangsfeldstärke dem daraus resultierenden Verbindungsabbruch durch automatisches Zurückschalten der Datenrate vorgebeugt wird. Sinkt der Empfangspegel von Client oder Access Point (AP) wird die Datenrate automatisch reduziert.

Beacon Interval Beacons sind Pakete, die ein Wireless Access Point sendet, um das WLAN zu synchronisieren. Das geschieht standardmäßig in einem Intervall von 100 Millisekunden.

Bridge Gerät, das zwei LAN-Segmente miteinander verbindet, die von gleicher oder von unterschiedlicher Art sein können wie beispielsweise Ethernet und Token Ring.

BSS ID Bei der BSS ID (basic service set identifier) handelt es sich um die eindeutige Kennung eines drahtlosen Netzwerkes mit einer Basisstation (Access Point). Sie wird im Access Point und auf allen Computern, die Zugriff auf dieses drahtlose Netzwerk haben sollen, eingestellt.

CRC CRC (Cyclic redundancy check, daher häufig CRC) ist ein Verfahren zur Bestimmung eines Prüfwerts für Daten, um Fehler bei der Übertragung oder Duplizierung von Daten erkennen zu können. Vor Beginn der Übertragung bzw. Kopie eines Blocks der Daten wird ein CRC-Wert berechnet. Nach Abschluss der Transaktion wird der CRC-Wert erneut berechnet. Anschließend werden diese beiden Prüfwerte verglichen. CRCs sind so ausgelegt, dass Fehler bei der Übertragung der Daten, wie sie beispielsweise durch Rauschen auf der Leitung verursacht werden könnten, fast immer entdeckt werden. CRCs können jedoch nicht die Integrität der Daten bestätigen.

CCMP CCMP oder auch Counter-Mode/CBC-Mac Protocol ist gemäß IEEE 802.11i ein Kryptographie-Algorithmus.

DBPSK Differential Binary Phase Shift Keying - IEEE 802.11 konformes Modulationsverfahren für Datenraten bis 11 Mbps. Dabei wird die Phase einer Sinusschwingung (Träger) durch Phasenverschiebung moduliert.
Entsprechend dem Binärwert (0 oder 1) eines Bits wird die Phasenlage der Sinusschwingung geändert. Die Frequenz dieser Schwingung wird Trägerfrequenz genannt.

DHCP Das DHCP (Dynamic Host Configuration Protocol) ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter an Computer in einem Netzwerk (z.B.

	Internet oder LAN). Durch DHCP ist die Einbindung eines neuen Computers in ein bestehendes Netzwerk ohne weitere Konfiguration möglich. Es muss lediglich der automatische Bezug der IP-Adresse am Client eingestellt werden. Ohne DHCP ist ein relativ aufwendiges Setup nötig, das neben der IP-Adresse die Eingabe weiterer Parameter wie Netzmaske, Gateway, DNS-Server, WINS-Server usw. verlangt. Per DHCP kann ein DHCP-Server diese Parameter beim Starten eines neuen Computers (DHCP-Client) automatisch vergeben.
Direct Sequence Spread Spectrum (DSSS)	Direct Sequence Spread Spectrum (DSSS) ist ein Frequenzspreizverfahren für die drahtlose Datenübertragung. DSSS ist (je nach Chipping-Sequenz-Länge) sehr gut gegen Abhören gesichert; das Signal verschwindet für Angreifer im Hintergrundrauschen. Je länger die Chipping Sequenz desto mehr Bandbreite wird benötigt.
DNS	DNS (Domain Name System) - Eine hierarchische verteilte Datenbank, die Zuordnungen von DNS-Domänennamen zu verschiedenen Datentypen, beispielsweise IP-Adressen, enthält. DNS ermöglicht das Suchen von Computern und Diensten anhand von benutzerfreundlichen Namen und ermöglicht außerdem die Suche nach anderen in der Datenbank gespeicherten Informationen.
ESS ID	Um mehrere drahtlose Netzwerke, mit je einem Access Point, zu einem drahtlosen Netzwerk zu verbinden, stellt man auf allen Access Points die gleiche Kennung ein. Diese wird dann als ESS ID (extended basic service set identifier) bezeichnet.
Firmware	Unter Firmware versteht man Software, die in Computer, Routern, Switche usw. in einem Chip integriert ist. Die Firmware ist heute meistens in einem Flash-Speicher oder einem EEPROM gespeichert. Sie enthält meistens elementare Funktionen zur Steuerung des Gerätes, sowie Ein- und Ausgaberoutinen.
Fragmentation Threshold	Die Fragmentierungs-Schwelle entscheidet, ob Pakete zerteilt werden, bevor sie drahtlos übermittelt werden. Sollten Sie eine hohe Paketfehlerrate feststellen, können Sie den Wert etwas veringern. Wenn Sie den Wert zu gering wählen, werden sie eine schlechte Übertragungsrate erreichen.

Frame	Frame ist die Bezeichnung der Dateneinheiten, die in einem Ethernet-Netzwerk auf Schicht 2 des OSI-Modells versendet werden. Dem Datenpaket werden Layer 2 Informationen (Ziel- und Absender-MAC-Adresse + Protokolloverhead) hinzugefügt und die Frame Check Sequence (Prüfsumme) wird hinten angefügt.
Hexadezimal	Hexadezimal bedeutet auf der Basis 16. Das Zahlensystem mit der Basis 16 wird zur Kurzdarstellung von Binärzahlen verwendet.
Hub	Zentrales Anschlussgerät in einem Netzwerk, das Kommunikationsleitungen in einer Sternkonfiguration miteinander verbindet.
IAPP (inter access point protocol)	Mit dem IAPP-Protokoll ist in WLANs eine standardisierte Kommunikation zwischen den Access Points (AP) möglich, die über Bridges miteinander verbunden sind. Das IAPP-Protokoll, das in 802.11f beschrieben ist, erweitert die beiden Standards IEEE 802.11a und 802.11g um das Roaming mobiler Clients über mehrere WLAN-Zellen hinweg. Das IAPP-Protokoll soll die Interoperabilität von Zugangspunkten verschiedener Hersteller verbessern, und damit proprietäre Lösungen überflüssig machen.
IEEE 802.11b / g	IEEE 802.11b ist die Bezeichnung für einen Wireless-Lan - Standard mit einer Übertragung im 2,4-GHz-Bereich. Im 2,4-GHz-ISM-Frequenzband stehen 14 Kanäle mit jeweils 22 MHz Bandbreite zur Verfügung. In Deutschland sind 13 Kanäle freigegeben, in den USA und Kanada 11, in Frankreich allerdings nur 4 ohne Einschränkung und weitere 9 Kanäle mit einer zusätzlichen Begrenzung der Sendeleistung. Es werden Datenraten bis zu 11 Mbit/s erreicht. Dabei ist zu beachten, dass sich diese Kanäle teilweise überlappen und daher in Deutschland nur 3 Kanäle ohne gegenseitige Beeinflussung zur Verfügung stehen. Der Nachfolger von IEEE 802.11b ist IEEE 802.11g mit Übertragungsraten bis zu 54 Mbit/s.
Infrastruktur	Im Infrastruktur-Modus wird eine Basisstation, häufig ein Wireless Access Point, speziell ausgezeichnet. Er koordiniert die einzelnen Netzknoten. Häufig ist diese Basis-Station dann auch Mittler in ein weiteres Netz, das sowohl Funknetz als auch ein klassisches Kabelnetz sein kann.

IP-Adresse Eine 32-Bit-Adresse zur Identifizierung eines Knotens in einem IP-Netzwerk. Jedem Knoten im IP-Netzwerk muss eine eindeutige IP-Adresse zugewiesen werden. Diese besteht aus der Netzwerkkennung und einer eindeutigen Hostkennung. Die Adresse wird in der Regel durch die Dezimalwerte der einzelnen Oktette, getrennt durch Punkte, dargestellt (beispielsweise 192.168.7.27). Unter dieser Version von Windows können Sie die IP-Adresse statisch oder dynamisch durch DHCP konfigurieren.

LAN Ein Kommunikationsnetzwerk, in dem eine Gruppe von Computern, Druckern und anderen Geräten, die sich innerhalb eines relativ begrenzten Bereichs (z. B. einem Gebäude) befinden, miteinander verbunden sind. In einem LAN kann ein Datenaustausch zwischen allen verbundenen Geräten im Netzwerk stattfinden.

MAC-Adresse Die MAC-Adresse (Media Access Control, auch LAN-Adresse genannt) ist die Hardware-Adresse vieler Netzwerkgeräte, die zur eindeutigen Identifikation des Geräts im Netzwerk dient. Die MAC-Adresse wird der Sicherungsschicht, Schicht 2 des OSI-Modells, zugeordnet.

Passwort Eine Passworteingabe ist ein Anmeldeverfahren zur Authentifizierung eines Benutzers innerhalb eines Systems, der sich durch eine eindeutige Information (das Passwort) dem System gegenüber ausweist. Zugriff auf das System erlangt nur der Benutzer welcher das korrekte Passwort eingibt. Dieses Verfahren schützt vor unberechtigtem Zugriff, wobei die Passwortlänge und die Zeichenkette eine entscheidende Rolle bei der Sicherheit darstellt. Je länger ein Passwort, je kryptischer (Passwort zusammengesetzt aus nicht logisch aufeinander folgenden alphanumerischen Zeichen), desto schwerer der unberechtigte Zugriff.

Peer - to - Peer Kommunikation, bei der beide Seiten gleich verantwortlich sind für Initiierung, Aufrechterhaltung und Beendigung der Session.

PING (Packet InterNet Groper) - Utility, mit der festgestellt werden kann, ob ein TCP/IP - Gerät zur Verfügung steht und in einem Netzwerk oder einer Internet-Site reagiert.

Radius	(engl. Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das zur Authentifizierung und Autorisierung von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient. RADIUS ist der de facto Standard bei der zentralen Authentifizierung von Einwahlverbindungen über Modem, ISDN, VPN, Wireless LAN oder DSL. Ein spezieller Server-Dienst, der RADIUS-Server, dient dabei der Authentifizierung von Clientgeräten oder Diensten gegen unterschiedliche Datenbanken, in denen die Zugangsdaten (zum Beispiel Benutzername und Passwort) gespeichert sind.
RJ - 45	RJ-xx ist die Abkürzung für von der US-amerikanischen Federal Communications Commission (FCC) genormte elektrische Steckverbindungen. RJ steht für Registered Jack (genormte Buchse). Folgende Typen sind die bekanntesten: RJ-11, RJ-12 und RJ-14 (vier- bzw. sechspolig), sowie RJ-45 (achtpolig), der im Netzwerkbereich zum Einsatz bei Twisted Pair - Netzwerkkabeln kommt.
Roaming	Roaming bezeichnet die Nutzung eines Kommunikationsendgerätes oder auch nur die Nutzung der Teilnehmeridentität in einem anderen Netzwerk (visited network) als dem Heimatnetzwerk (home network). Hierzu ist erforderlich, dass die Betreiber der beiden Netzwerke ein Roamingabkommen getroffen haben sowie die erforderlichen Signalisierungs- und Datenverbindungen zwischen ihren Netzen geschaltet haben.
Router	Computersystem, das Datenpakete speichert und weiterleitet - über Netzwerkadressen - von einem LAN oder WAN zum nächsten.
RTS Threshold (request to send threshold)	Sendeanforderungs-Schwellenwert - Die Sendeanforderung wird sowohl bei Modem-Steuerungen benutzt als auch beim kollisionsfreien LAN-Zugangsverfahren CSMA/CA, wie es in 802.11 eingesetzt wird. Der chwellwert wird in Byte angegeben. Jedes Datenpaket das diesen Werte überschreitet, löst den RTS/CTS Mechanismus aus, um eine bevorzugte drahtlose Übertragung zu erreichen.
SMA-Anschluss	SMA-Anschlüsse werden für Antennenanschlüsse in Frequenzbereichen von 1GHz bis 18 / 26,5 GHz eingesetzt. Reverse-SMA Anschlüsse findet man hingegen an Wireless LAN Geräten. Beide Anschlussarten sehen gleich aus.

Sie sind aber vom Innenaufbau grundverschieden und können nur in ihrem definierten Einsatzbereich benutzt werden.

Subnetzmaske Ein 32-Bit-Wert, mit dem der Empfänger von IP-Paketen die Netzwerkkennung in einer IP-Adresse von der Hostkennung in der IP-Adresse unterscheiden kann. Subnetzmasken haben in der Regel das Format 255.x.x.x.

Switch Ein Switch ist im Prinzip eine Multiport Bridge und somit eine aktive Komponente im Netzwerk, die auf Schicht 2 eines Ethernet LANs arbeitet. Sie dienen als Konzentrator in Netzwerken mit Sterntopologie. Den Kern eines Switches bildet dabei die Switching Fabric, welche die Performance bestimmt. Darüber hinaus kennzeichnen die Forwarding Rate (maximale Anzahl an Datenpaketen, die pro Sekunde) und die Filtering Rate (maximale Anzahl der bearbeiteten Datenpakete und verwaltbaren MAC-Adressen) die Leistungsfähigkeit eines Switches. Switches werden außerdem nach dem Schaltverfahren unterschieden; diese sind Cut Through, Fragment Free und Store and Forward. Bei Cut Through werden die Datenpakete, um die Verzögerungszeit in dem Switch so kurz wie möglich zu halten, einfach durchgeschleust. Nachdem die Zieladresse ermittelt wurde, wird nicht die vollständige Übertragung der Daten abgewartet, sondern gleich weitergeleitet. Für dieses Verfahren sind, neben der Zieladresse keine weiteren Informationen, die in dem Paket enthalten sind, wichtig. Dadurch kann die Verzögerungszeit drastisch reduziert werden. Bei dem Fragment-Free-Verfahren wird ein bestimmtes Zeitfenster abgewartet, um Kollisionen im Zielsegment zu vermeiden. Das geläufigste Verfahren ist jedoch das Store-and-Forward-Verfahren bei welchem die Daten in dem Svvitch zwischengespeichert werden, bevor sie weitergeleitet werden. Der Vorteil dieses Verfahrens ist, dass die Daten eine Fehlererkennung und Fehlerkorrektur durchlaufen, wohingegen der Nachteil einer größeren Verzögerungszeit besteht.

TCP/IP Transmission Control Protocol/Internet Protocol (TCP/IP) - Eine Gruppe von im Internet häufig verwendeten Netzwerkprotokollen, die die Kommunikation über miteinander verbundene Netzwerke aus Computern mit unterschiedlichen Hardwarearchitekturen und Betriebssystemen möglich macht. TCP/IP umfasst

	Standards für die Kommunikation zwischen Computern und Konventionen zum Verbinden von Netzwerken sowie zum Routing des Datenverkehrs.
TKIP	Das Temporal Key Integrity Protocol (TKIP) wird von den Standards 802.1X und WPA für die Authentifizierung verwendet. Dieses von Verschlüsselungsspezialisten entwickelte Protokoll legt sich um WEP und soll so dessen Sicherheitslücken schließen.
Web-Browser	Software, die den HTML-Code in Dateien verarbeitet, zu Webseiten formatiert und für den Endbenutzer anzeigt. Einige Browser ermöglichen es Benutzern auch, E-Mail-Nachrichten zu senden und zu empfangen, Newsgroups zu lesen und in Webdokumenten eingebettete Audio- oder Videodateien wiederzugeben.
WEP	Teil des WLAN-Standards IEEE 802.11 ist Wired Equivalent Privacy (WEP), ein Sicherheitsstandard, der den RC4-Algorithmus enthält. Eine Verschlüsselung mit nur 40 Bit bzw. 104 Bit ist enthalten.
Wireless LAN	(Wireless Local Area Network) - Drahtloses Kommunikationsnetzwerk, das Computer, Drucker, Notebooks, Router und andere Geräte per Funk miteinander verbindet. Gängige Standards sind IEEE.802.11b (Datenübertragungsrate max. 11MBit/s) und IEEE.802.11g (Datenübertragungsrate max. 54 Mbit/s).
WPA	Wi-Fi Protected Access (WPA) ist eine Verschlüsselungsmethode für ein Wireless LAN. Nachdem sich die Wired Equivalent Privacy (WEP) des IEEE-Standards 802.11 als unsicher erwiesen hatte und sich die Verabschiedung des neuen Sicherheitsstandards 802.11i verzögerte, wurde durch die Wi-Fi eine Teilmenge von 802.11i vorweggenommen und unter dem Begriff WPA als Pseudostandard etabliert. WPA bietet zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren, und bietet zur Authentifizierung von Nutzern PSK (Pre-Shared-Keys) oder Extensible Authentication Protocol (EAP) über 802.1x an. WPA basiert auf dem RC4 Stromchiffre welcher schon für WEP genutzt wurde. Im Gegensatz zu WEP nutzt WPA nicht nur einen 48-bit langen IV (Initialisierungsvektor) (bei WEP nur 24-bit lang), sondern auch eine per-packet key mixing Funktion,

einen re-keying Mechanismus, sowie einen Message Integrity Check (MIC) namens Michael. Die Authentifizierung über EAP wird meist in großen Wireless LAN genutzt.

WPA 2

Wi-Fi Protected Access 2 (WPA2) ist ein Sicherheitsstandard für Funknetzwerke nach den Standards IEEE 802.11a, b und g. Er basiert auf dem Advanced Encryption Standard (AES) und stellt den Nachfolger von WPA dar und implementiert die grundlegenden Funktionen des neuen Sicherheitsstandards IEEE 802.11i. WPA2 nutzt den Verschlüsselungsstandard AES. Zwei weitere Verschlüsselungsprotokolle wurden bei WPA2 hinzugefügt: TKIP und CCMP, welches nun auch WPA2 im Ad-hoc-Modus ermöglicht. WPA2 und WPA können gemeinsam eingesetzt werden, sofern WPA2 vom Access Point unterstützt wird. WPA2 und WEP können nur bei wenigen speziellen Access Points gemeinsam verwandt werden. Alle Geräte die für WPA2 von der Wi-Fi Alliance zertifiziert werden sollen, müssen den Standard IEEE 802.11i erfüllen. WPA2 erfüllt die strengen Sicherheitsvorschriften für Datenaustausch in US-Behörden nach FIPS 140-2.